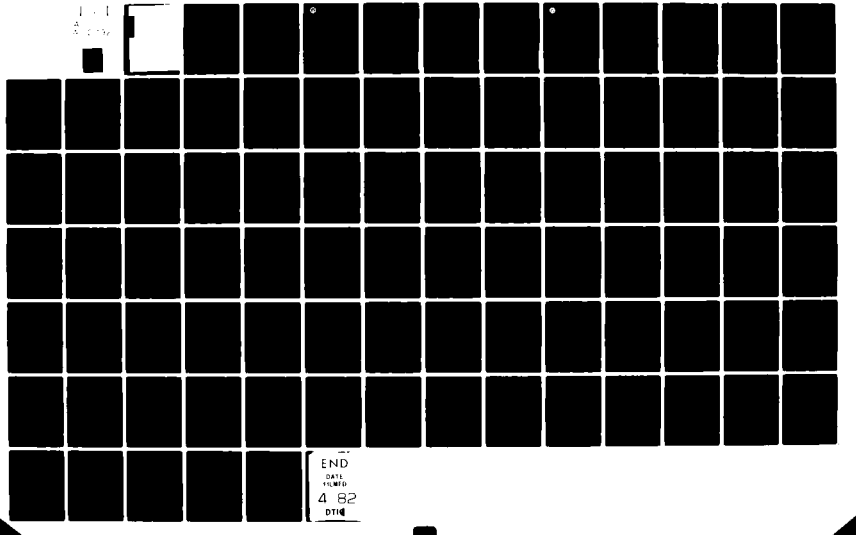
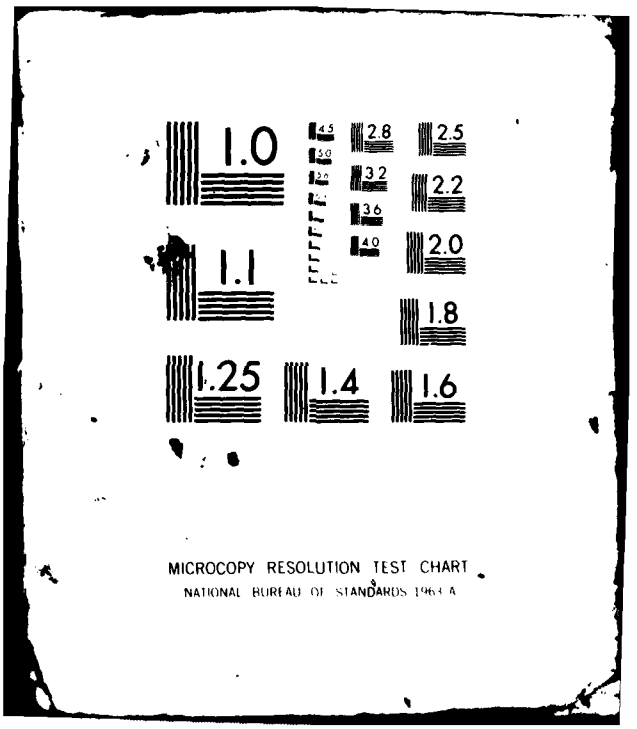
AD-A112 792 NAVAL RESEARCH LAB WASHINGTON DC F/G 17/2
MILITARY MESSAGE EXPERIMENT. VOLUME II.(U)
APR 82 S H WILSON, N C GOODWIN, E H BERSOFF
UNCLASSIFIED NRL-MR-4456-VOL-2 NL



END
DATE FILMED
4 82
DTIC


1.0
1.1
1.25
1.4
1.6
2.8
3.2
3.6
4.0
2.5
2.2
2.0
1.8
MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS 1963 A

(c) determine the training requirements associated with the introduction

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE	READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER NRL Memorandum Report 4456	2. GOVT ACCESSION NO. AD-A112 792	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) MILITARY MESSAGE EXPERIMENT FINAL REPORT — VOL. II	5. TYPE OF REPORT & PERIOD COVERED Final report 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) S. H. Wilson, N. C. Goodwin*, and E. H. Bersoff**	8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Research Laboratory Washington, DC 20375	10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS 64510N; X-0743-CC; 0103-0-0
11. CONTROLLING OFFICE NAME AND ADDRESS	12. REPORT DATE April 1, 1982 13. NUMBER OF PAGES 86
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)	15. SECURITY CLASS. (of this report) UNCLASSIFIED 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution unlimited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

*The MITRE Corporation **CTEC, Inc.

Prepared in cooperation with the Naval Electronic Systems Command, Naval Telecommunications Command, Information Sciences Institute of the University of Southern California, and the Defense Advanced Research Projects Office.

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

MME	Security kernel
AMH	SIGMA
Message system	COTCO
Security	DISTAN

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

The Military Message Experiment (MME) was designed to evaluate the utility of user-oriented message processing systems in a military environment and to aid in determining the features useful in such a system. The experiment was a cooperative effort between the Commander-in-Chief, Pacific, the Navy, and the Defense Advanced Research Projects Agency. To conduct the experiment, a PDP-10-based system was installed at CINCPAC Headquarters for use by a portion of the Operations directorate. The

(Continues)

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

20. ABSTRACT (Continued)

message processing functionality was provided by SIGMA, a program written by the Information Sciences Institute of the University of Southern California. It was supported by the TENEX operating system, and the user terminals were modified HP-2649A CRTs.

The MME system was designed to give the user the capability to handle his message traffic (both incoming and outgoing, formal and informal) on the system. The system enforced multilevel security rules based on a modification of the security kernel model developed at Mitre. The rule enforcement was not rigorous enough for certification, but it was sufficiently rigorous to determine the effects on the users' interactions with the system. Most of the functions needed for a user's message-related tasks were provided by the system: message filing, message replies, message commenting and "chopping;" and message release.

The following conclusions were reached as a result of the experiment:

a. An Automated Message Handling System (AMHS) can be extremely useful in a military environment, especially during a crisis. It must be extremely reliable and routinely available.

b. There are not significant differences between message system requirements in normal and crisis operation. During a crisis, the system must handle a higher volume of traffic. An AMHS will be effective during a crisis only if the personnel use it daily and are, thus, thoroughly familiar with its operation.

c. An AMHS must provide services to everyone involved with message handling. Each user may not have a terminal; thus, the system must have well thought-out procedures for including these individuals in procedures that have been automated (e.g., distribution).

d. An AMHS must have the capability to produce hardcopy. In the MME, many users preferred paper copies for reviewing messages and preferred manual to automated coordination.

e. An AMHS should be an integral part of the user's information handling system. Users who draft messages need to refer to many documents, including other messages, reports, and letters. Many of these may be stored on other automated systems, such as word processors and command and control systems. A single work station is needed to support all of these user functions.

f. An acceptable user interface can be developed based on the security kernel concept.

g. A user-oriented message system and the telecommunications center message system with which it is associated must be integrated. Failure to integrate these functions will result in reduced reliability and increased cost because of incompatible interfaces and duplication of functions.

h. An AMHS is a more complex program than is generally thought. It must exhibit the characteristics of a well-designed data base system, a user-oriented message processor, an interactive command and control system, and a rapid message handling system.

DEPARTMENT OF THE NAVY

From: Commander, Naval [illegible]
To: Distribution List
Via: Commander, Naval Telecommunications Command

Subj: Military Message Experiment (MME)

Ref: (a) MME Memorandum of Agreement of May 1978
(b) COMNAVELEX ltr Ser 33-310 of 6 Mar 1979
(c) COMNAVELEX ltr Ser 370-310 of 2 Nov 1979

Encl: (1) MME Final Report (Volumes I, II, III)

1. Enclosure (1) is submitted as the final report on the Military Message Experiment (MME) conducted at Commander-in-Chief Pacific (CINCPAC) Headquarters, Camp Smith, Hawaii, in accordance with the agreement of reference (a). Volume I provides an Executive Summary of the Experiment, Volume II presents the detailed final report, while Volume III presents the comments on the Experiment and the military utility of the message systems. References (b) and (c) previously submitted the Experiment "Quick-Look" and "Mid Experiment" reports.

2. The Experiment was a mutual effort of [illegible] Advanced Research Projects Agency; Naval [illegible] Command; and Naval Electronic Systems Command [illegible] was assigned responsibility for the evaluation of the [illegible] and the preparation of this final report.

3. Measuring the utility to a major command staff of [illegible] Message Handling System has been a difficult task. It was recognized at the outset that evaluating the MME, as a computer-based message/information [illegible] difficult, but the interaction of [illegible] hardware reliability, security [illegible] the coordination requirements between [illegible] J3 and J4) were not fully understood [illegible] fully appreciated. The technical [illegible] them, and the CINCPAC staff took many [illegible] example, in Volume III, General [illegible] staff, who arrived after the MME was [illegible] more positive view of it than those who [illegible] growing pains.

Subj: Military Message Experiment (MME)

4. Automated aids for command staffs will have significant impact in their ability to fight a war. The complexity of this [illegible] highlights the need for carefully thought out systems [illegible] inadequate or poorly designed system may hurt [illegible] all. The Overview of Volume I provides a concise summary of the MME. Volume I provides a more detailed Executive Summary that covers the major points of the experiment for those persons who only require a high-level summary of the subject. Anyone involved deeply in such programs is urged to read at least Volumes I, II, and III carefully.

5. The submission of this final report concludes the Military Message Experiment. Volumes IV through VII provide further supporting data and analysis and may be obtained separately.

J. S. LAWSON, JR.
By direction

Distribution:
(See page 3.)

Subj: Military Message Experiment (MME)

Distribution:
OUSDRE (C^{3}I) Information Systems (Mr. Walter) (2)
JCS (J3-ISD) (2)
DCA (Code 534) (3)
DARPA (IPTO) (2)
CNO (OP 094) (3)
CINCPAC (J3) (3)
CINCPAC (J6) (3)

Copy to:
House Appropriations Committee (Mr. Robert Seraphin)
National Bureau of Standards (Dr. S. Kimbleton)
National Science Foundation (Mr. P. Custer)
CINCLANT
CINCMAC
CINCPAC (J5311) (2)
CINCSAC
CINCAD
HQ SAC (DXT)
CCTC (Code C634)
CDR USACC (CC-OPA-WA & CC-OPS-T)
CDR7THSIGCOMD (CCN-PO-NO)
DA (DACC-SIF) (2)
DCEC (Code B-800) (2)
DDC
DIA (RSO-3&RSP-2) (2)
Dir. DARPA Regional Office, Europe
HQ TRADOC (ATCD-C-C)
SHAPE (Mr. W. Stoney)
USCINCEUR (ECJ3-OD, WSEO-E) (2)
USCINCRED
USREDCOM (ECJ6-T)
USCINCSO
WSEO/DCA (COL Pixton, MAJ Nell) (2)
PTAO
NADC (Dr. E. Plante)
CINCUSARMYEUROPE (ODCSOPS-DPLE)
OPNAV (OP 942P, OP 941)
USNPGS (Code 1424, Library) (2)
NAVDEASYSCOM (Code 047)
COMNAVTELCOM
COMNAVELEXSYSCOM (PME 107-3C, PME 110, PME 120, PME [illegible])
NISSBA (3)
NSWC (Code 8122) (2)
NRL (Code 7590)
NOSC (Code 100, 437) (2)
(Continued on page 4.)

Subj: Military Message Experiment (MME)

Copy to: (continuation)
HDQPACAF (DCS OPS & INT)
HDQUSEUCOM (LCDR Byard)
HQ USAF (AF/XOKCR) (3)
Dept. AF (Prog. Dir., TARMS, Dept. for Comm. & Inf. Systems; HDQ ELEX SYS DIV; LT Ringo) (2)
Dept. AF AFCCPC (MAJ R. Harris)
AFLS/IND (Mr. W. Lamour)
BBN Information Mgt. Corp. (Dr. McQuillan)
CTEC (Dr. Bersoff)
IBM (Mr. J. Gould)
IBM Research Laboratory (Mr. J. Bennett)
Information Sciences Institute (Mr. K. Uncapher)
ITT Europe Eng. Support Centre (B. M. Drake)
Logicon, Inc. (Seal Hayes)
MITRE Corporation
MITRE Corporation (Mr. J. Mitchell)
System Development Corporation (IAIPS)

DEPARTMENT OF THE NAVY

FIRST ENDORSEMENT on Commander, Naval Electronics Systems Command
126/06T of 23 Dec 81

From: Commander, Naval Telecommunications Command
To: Distribution List

Subj: Military Message Experiment (MME)

1. Forwarded

2. This final report on the Military Message Experiment (MME) closes the book on a unique, experimental message handling system which was installed in the operational environment of a major joint commander during the period May 1978 - September 1979. The MME demonstrated that an automated message handling system could be a valuable asset to a major staff. Indeed, recent progress in the fields of word and distributive processing are such that operational systems for major staffs are foreseen as a forthcoming reality. Therefore, the experience gained and lessons learned during the MME should be considered in the development of any future automated message handling systems.

R. H. Conley

Distribution:
(See Page 2)

Subj: Military Message Experiment (MME)

Distribution:
OUSDRE (C^3I) Information Systems (Mr. Walker) (2)
JCS (J3-ISD) (2)
DCA (Code 534) (3)
DARPA (IPTO) (2)
CNO (OP 094) (3)
CINCPAC (J3) (3)
CINCPAC (J6) (3)

Copy to:
House Appropriations Committee (Mr. Robert Seraphim)
National Bureau of Standards (Dr. S. Kimbleton)
National Science Foundation (Mr. F. Custer)
CINCLANT
CINCMAC
CINCPAC (J5311) (2)
CINCSAC
CINCAD
HQ SAC (DXT)
CCTC (Code C634)
CDR USACC (CC-OPA-WA & CC-OPS-T)
CDR7THSIGCOMD (CCN-PO-NO)
DA (DACC-SIF) (2)
DCEC (Code R-800) (2)
DDC
DIA (RSO-3&RSP-2) (2)
Dir. DARPA Regional Office, Europe
HQ TRADOC (ATCD-C-C)
SHAPE (Mr. W. Stoney)
USCINCEUR (ECJ3-OD, WSEO-E) (2)
USCINCRED
USREDCOM (RCJ6-T)
USCINCSO
WSEO/DCA (COL Pixton, MAJ Neil) (2)
FTAG
RADC (Dr. K. Pisare)
CINCUSARMYEUROPE (ODCSOPS-DPLE)
OPNAV (OP 942F, OP 941)
USNPGS (Code 1424, Library) (2)
NAVSEASYSCOM (Code 04?)
COMNAVTELCOM
COMNAVELEXSYSCOM (PME 107-30, PME 110, PME 120, PME 136, ELEX [illegible]
NIPSSA (3)
[illegible] (Code [illegible]) (2)
[illegible] (Code 7590)
[illegible] (Code 100, 437) (2)
[illegible]

[illegible]

[illegible]
[illegible]
[illegible]
[illegible] (OP/[illegible]) [illegible]
[illegible] (Comd. [illegible], [illegible] Dept. for Comm. & Inf. [illegible]
[illegible] (2)
[illegible] AFCCPC (MAJ [illegible])
[illegible] (Mr. V. [illegible])
[illegible] Information Mgt. Corp. (Mr. McQuillan)
[illegible] (Mr. [illegible])
[illegible] (Mr. J. Gould)
[illegible] Research Laboratory (Mr. J. Bennett)
Information Sciences Institute (Mr. K. Uncapher)
[illegible] Europe Eng. Support Centre (S. M. Drake)
[illegible], Inc. (Neal Hayes)
[illegible] Corporation
[illegible] Corporation (Mr. J. Mitchell)
System Development Corporation (IAIPS)

CONTENTS

LIST OF TABLES AND FIGURES

MILITARY MESSAGE EXPERIMENT
FINAL REPORT

SECTION 1
BACKGROUND

1.1 Introduction

During the late 1960s, two American ships, the USS Liberty and the USS Pueblo, were involved in separate crises. Each crisis was exacerbated by unacceptably long delays in the delivery of critical military messages. Members of Congress investigated the quality of U.S. military communications [1-4] and identified several causes for the delays. Further, they noted that there were numerous, apparently uncoordinated, military message centers under development by various elements of the Department of Defense. This resulted in a memorandum from the Director, Telecommunications and Command and Control, OSD, in June 1975, directing that techniques needed for secure interactive message systems be developed. This directive, and parallels between message processing systems being developed by the Department of Defense Advanced Research Project Agency (DARPA) and emerging user requirements within military staffs, led to a Memorandum of Agreement (MOA) [5] between DARPA, the Naval Telecommunications Command (NAVTELCOM), Naval Electronic Systems Command (NAVELEXSYSCOM), and the Commander in Chief Pacific (CINCPAC) for the conduct of a military message experiment (MME).

The concept of the MOA was to determine the need for and type of future automation in the handling of military messages and to define an experiment to validate message processing requirements. Under the MOA, DARPA was given general responsibility for the development of the MME System; NAVTELCOM acted as the single point of contact for the Navy; NAVELEXSYSCOM had responsibility for evaluation of the MME; and CINCPAC had general responsibility for providing the experiment environment, services, personnel, and support facilities.

The specific objective of the MME was to determine the utility of an interactive message service in a major military headquarters. As a part of this determination, alternative features and capabilities were to be identified; the use of the features was to be observed and measured as a means of determining the requirements that staff officers and action officers have for automation of message systems. These requirements are to be used as a baseline for developing automated message handling systems for future military use. Accordingly, the specific objectives identified in the MOA were to:

(a) determine and demonstrate the usefulness of automated message capabilities and the necessary features to support a military message handling system in an operational environment;

(b) determine the effect of an automated message handling system on operational procedures, manpower, and logistics in an operational environment;

Manuscript submitted December 19, 1980.

(c) determine the training requirements associated with the introduction of an automated message handling system;

(d) determine the characteristics of an acceptable user interface for an interactive automated message handling system;

(e) determine multilevel security design characteristics and their impact on the user interface; and

(f) obtain the data necessary to assist in the future design and development of a family of automated messsage handling systems for DOD use.

1.2 Report Structure

The Final Report of the Military Message Experiment is structured as a series of volumes--published both individually and jointly by participating organizations. The following table lists the volumes of the report.

TABLE 1. MME Final Report Volumes

Volume Number	Objectives Discussed	Topic	Authors' Affiliations
I	(a)-(f)	Executive Summary [6]	Naval Research Laboratory The MITRE Corp. CTEC, Inc. Naval Electronic Systems Command
II	(a)-(f)	Final Report	Naval Research Laboratory The MITRE Corp. CTEC, Inc.
III	(a),(b) (c),(f)	CINCPAC's User View [7]	CINCPAC
IV	(a),(b)	Message System Utility [8]	Naval Research Laboratory
V	(a),(d) (f)	ISI's Developer View [9]	Information Sciences Institute
VI	(a),(b)	Data Analysis [10]	The MITRE Corp.
VII	(c)	Training [11]	The MITRE Corp.

Volumes I-III describe the basic experiment and its results. The remaining volumes present supporting data and analyses for volumes I-III. The preceding table indicates the principal experimental objectives that are discussed in each of the volumes.

1.3 System Selection

Organizations under contract to DARPA were chosen to modify their work on interactive message systems so that the systems could be used by military personnel to send and receive messages via the AUTODIN system. Preliminary designs for these "militarized" versions of three candidate message systems were submitted by Bolt, Beranek, and Newman Inc. (BBN), the Massachusetts Institute of Technology (MIT), and the Information Sciences Institute (ISI) of the University of Southern California. In order to aid the developers in tailoring their system to the military environment, a set of capabilities needed for a secure military message processing system was developed by DARPA, Navy, and contract personnel [12,13]. During the period 22 February through 3 March 1977, representatives from the Navy, DARPA, MITRE Corp., CTEC, Inc., and the CINCPAC staff evaluated the three candidate message systems.

The evaluators concluded that SIGMA, the message service developed by USC-ISI, presented the user with an interface and features that would allow the most useful data to be derived from the experiment, but noted that SIGMA, at that time, could not adequately support the experiment and that there was "a considerable risk in upgrading the performance of SIGMA to an acceptable degree." The "performance" of the system referred to the time needed for the system to respond to and execute an instruction entered by a user. See Section 3 of this report for a discussion of the steps taken to improve SIGMA's performance. A plan was developed to improve performance and the features related to security and message handling based on the evaluation. At the conclusion of the evaluation (documented in [14,15]) SIGMA was selected and subsequently installed as a part of the MME system at CINCPAC in May 1977.

1.4 System Composition

The basic elements of the MME system as used in the experiment included:

(a) Hardware: a DEC PDP-10 computer with TENEX operating system installed in a TOP SECRET facility with on-line connection to the AUTODIN system via the Local Digital Message Exchange (LDMX), a terminal interface processor (PDP-11) 25 user terminals and 7 printers located in the J3 office areas of CINCPAC.

(b) Software: a message service software system (SIGMA) installed on the PDP-10 and a terminal interface system and LDMX interface system installed on the PDP-11.

(c) Experiment Support Staff: system operators, technicians, training and management personnel.

1.5 System Overview

For a complete descripton of the features of SIGMA, see Vol V (ref [9]) of this series. For a brief description of some similar message-processing systems, see ref [16]. The following brief description is adapted from the SIGMA reference manual.

Users may draft messages on-line using standard message formats provided by SIGMA. Text processing features aid the user in composing and editing messages. The message review (chopping) procedures are automated so that draft messages are electronically distributed to the reviewers who may approve, disapprove, comment, and edit using SIGMA. The drafts are then returned by the system to be redrafted or released. Although the procedures have been automated, the users may at any time obtain printed copies of any information in the system.

Upon release, outgoing messages are delivered electronically to the AUTODIN system via the LDMX. Comeback copies are automatically sent to internal distribution lists. Likewise, messages received from AUTODIN are electronically routed by SIGMA (controlled in the experiment by the J3 administrative office). In addition to the formal record traffic, SIGMA provides two other types of messages for use within the command - formal memo and informal note. SIGMA provides on-line files similar in concept to the action officers' standard file cabinets and safes. Users may construct any number of on-line files and organize them in any manner they wish. These files may contain arbitrary numbers of entries.

In addition to these personal files, users are automatically assigned other special files. Associated with each office code are files containing entries for messages and drafts awaiting attention; the entries are placed there automatically by SIGMA. These files are called PENDING files. Similarly, each user has a file for his own personal use called MYPENDING. Files may be defined to be used as READBOARDS such that they may be accessed by all the necessary office codes. Finally, there is an ACTION LOG, a file used to track ACTION assignments and accomplishments related to messages.

In addition to messages and files of message entries, SIGMA provides for the storage of arbitrary text. For example, users may construct personal addressee ACTION and INFO lists as text and insert them into the chop list of a draft message.

1.6 System Operations and Reports

Operations in connection with the MME began at CINCPAC in May 1977 and ended in September 1979. During this period, members of the Operations Directorate (J3) at CINCPAC Headquarters, Camp Smith, Hawaii, used the computer system for receiving, redistributing, filing, and retrieving incoming messages. The system was also used for the generation, coordination, and release of outgoing AUTODIN messages and the creation and distribution of

formal and informal notes and memoranda. Specific activities in each of these areas are discussed in this final report.

This report summarizes activity at CINCPAC during that period, identifies conclusions drawn on the basis of that activity, and discusses potential implications for future automated message handling systems. Two previous reports cover earlier phases of the experiment in detail. The Quick Look Report [17] discusses the inception and early operation of the system during the period May 1977 to October 1978 and provides a summary of the SIGMA message service software which served as the basis for user interaction with the MME System. Additional SIGMA details can be found in [18-21]. A second report, the Mid-Experiment Report [22] covers operational activity during the period November 1978 to April 1979 and provides a discussion of the telecommunications interface aspects of the experiment. This Final Report covers the period of Full Experimental Use, from February 1979 through the end of the experiment in September 1979. In addition, it summarizes the entire experiment.

SECTION 2
SECURITY

2.1 Introduction

One of the major goals of the experiment was to determine the feasibility of implementing a secure message processing system. The two major requirements for a secure system are to ensure that:

(a) users cannot gain access to information for which they are not cleared and

(b) the security classification of information in the system cannot be modified improperly.

The specific security requirements are detailed in [12] and [13]; the results of the evaluation of the security design of the three candidates' message processing systems are contained in [15]. The specific requirements were to:

(a) provide non-discretionary controls to enforce the DoD security policy;

(b) provide discretionary controls for file access by individuals, organizations, groups of individuals, subgroups, and combinations thereof;

(c) provide an acceptable user interface;

(d) include message release as part of security controls;

(e) provide multilevel message files;

(f) provide a rich interface (useful functions to read audit trails, change passwords, review files, summarize activity statistics, etc.) for the system security officer to monitor and control the system;

(g) identify the security-relevant program modules and analyze the ramifications of granting write-down capabilities for certain modules;

(h) provide a capability for a user to downgrade information;

(i) keep the user aware of the classification of the information being displayed, printed, or entered;

(j) alert the user to possible security violations; and

(k) provide the user with a consistent view of the system when operating at different security levels.

2.2 Security Kernel Based Message Handling Systems

The final implementation did not satisfy all the goals, but the SIGMA message service represents a significant advance in the development of multilevel secure message systems. Although the service was implemented on the nonsecure TENEX operating system, the user interface was designed as though it were running on a security kernel with the the result that SIGMA's interface would remain unchanged if SIGMA were reconstructed to operate with a security kernel (see [23]). Currently, there are no other computer-based interactive message systems in use within DoD that have a multilevel secure user interface, i.e, an interface that reflects the restrictions imposed by a formal security policy.

Efforts to use formal security models for secure ADP systems include, among others, the Kernelized Secure Operating System (KSOS) [24], the Secure Communications Processor (SCOMP) [25], the Provably Secure Operating System (PSOS) [26], the ADEPT-50 time-sharing system [31], MULTICS [32], the Kernelized VM/370 (KVM/370) [33], and the capability-based system, GNOSIS [34]. For a more complete discussion of formal models for security, see [35]. Both KSOS and SCOMP are based on the construction of security kernels, similar to the one simulated in SIGMA. The term kernel is used because in both KSOS and SCOMP the programs that control the security are isolated from the rest of the programs and are contained in a security kernel. Hence, if a program that is not a part of the kernel fails, it will not have an adverse effect on security. The developers of KSOS and SCOMP plan for them to be verified mathematically to conform to a mathematical model [27] of the DoD security policy. Stated simply, the model consists of the following two rules:

(a) A subject (user or program operating on behalf of a user) cannot read information unless his security level is greater than or equal to the security level of the information - the simple security rule.

(b) A subject cannot lower the security level of information - the *-property (pronounced, the star-property).

Violation of the *-property would allow access to information by subjects with lower security levels. Advocates of the kernel technology claim that it will be possible to construct multilevel secure message systems based on these operating systems [28]. Early message system designs based on this security model led to an unacceptable user interface. Consequently, the rigid enforcement of the model was relaxed in some respects; see page 10 of the Quick Look Report [17].

2.3 Privacy Controls

Message systems may also be required to enforce privacy controls, i.e., controls that restrict message access to those persons who have some need to see a message. (We are not referring to the controls legislated in the Privacy Act of 1974.) Even with a SECRET clearance, a user is not allowed to read all information at SECRET or below: he is only permitted to view information for which he has a need-to-know. Additionally, a coordinator often wishes to prevent circulation of his comments concerning a message. While enforcement of privacy is desirable in systems that handle formal

messages, its importance to the DoD has been secondary to enforcement of security controls. This is largely due to the fact that preventing the unauthorized disclosure of classified information is easier than preventing violations of privacy.

2.4 SIGMA Security Architecture

The use of SIGMA has clarified some of the security issues. A key feature of SIGMA's secure user interface is a multilevel user terminal [21] with special function keys for security-relevant operations. The screen of the multilevel terminal is divided into several windows, each of which is a logically independent terminal. The windows scroll independently and may have different security levels. Each terminal contains two sets of security lights. One set indicates the security classification of the window in which the cursor is located and, thus, the classification the system will assign to any information the user types in. The second set of lights indicates the security level of the most highly classified information on the screen.

To define and support their secure interface, SIGMA designers developed a special software architecture [23]. A SIGMA user interacts with up to five different logical processes: a trusted process, an unclassified control process, and one process for each of the three levels of classified information that SIGMA supports. Each process other than the trusted process is constrained to write data only at its own level and to read data at its level or below. The trusted process is allowed to transfer information in a controlled manner from one security level to a lower level. Thus the trusted process may violate the *-property. Because of this capability, the trusted process would be subjected to close scrutiny in a message system being certified for multilevel secure operation.

2.5 Evaluation of User-Visible Security Features

It is important to evaluate the security model that was simulated by SIGMA according to the user-visible features. Those most obvious to the user were:

(a) log-on security level;

(b) multiple windows, security lights, and function keys;

(c) forced assignment of security level to each message at creation time;

(d) capability to reply to a message at a different security level;

(e) confirmations required when the trusted process violated the *-property;

(f) review of text for downgrading; and

(g) message release.

2.5.1 Log-On Security Level

The user logged on giving both a personal ID, possibly an organization code, and a maximum security level for that session. This session security level could be no higher than the lower of the maximum level for the particular terminal and the user's maximum. The user could not then have access to any information at a level higher than the session security level. Although most of the users always logged on at their maximum level, there were occasions when a user logged in at a lower level in order to restrict the classification level of the information displayed. In many installations, time-consuming manual procedures are used to "sanitize" the environment when visitors without top clearances are in the area. In SIGMA, a user could log in at a lower level so as to prevent the display of highly classified data on the screen. A user could also log in at a lower level when he wanted to be certain that only documents no higher then a certain level were included in a message or report.

2.5.2 Multiple Windows, Security Lights, and Function Keys

With the decreasing cost of computer technology, the capabilities of terminals will increase. The amount of programmable code in the terminal will increase to the point that the "computer security problem" will be manifest in the terminal as well as in the main processor. This could lead to the need for a security kernel within the terminal. Whether or not the requirement for a kernel in the terminal is as strong as for one in the main processor, there is an unquestioned need to reduce the amount of code in the terminal that can affect security. The purpose of both the security lights, which would be replaced by a small alphanumeric display in a future terminal, and the function keys was to simulate a direct communication between the user and the security kernel within the main computer. With such a channel, the software within the terminal cannot maliciously or inadvertently change the security of an object being displayed. The multiple windows provide a capability of displaying objects at different levels of classification simultaneously on the same display. User confirmation via a function key was required whenever any program in the system communicated with any other program at a lower security level, i.e., violated the *-property. The purpose of requiring the confirmation was to add an additional check to ensure that these special programs did not surreptitiously downgrade classified information.

Interviews with users at the end of the experiment indicated that few understood the security model enforced in the system and, thus, the functions of the security lights and the confirmation keys. The lack of understanding can be attributed to several things. First, because the system was not operating as early as was expected, the original trained users had rotated out of CINCPAC. Although new users were trained, the emphasis on security was not as great as in the initial training. Second, the users operated in a controlled TOP SECRET environment; therefore, they were not as conscious of security as users who must routinely open safes and deal with some people who are cleared and some who are not. Third, they had complete trust that computers would maintain the proper controls over classified material. (Security tests on other systems have shown that such faith is unwarranted in almost every case.)

Most users did not find the security controls imposed by the lights, windows, and function keys to be overly restrictive. Because many did not understand the role of the confirmation keys they thought they were an unnecessary bother.

2.5.3 Forced Assignment of Security Level at Message Creation

A design decision was that every object in the system must always have an assigned security classification. Thus, there were three design alternatives considered in the message creation process: a) default to system low (UNCLASSIFIED) with access restricted only to the creator until he assigned a classification, b) default to system high (TOP SECRET), or c) force the user to assign the proper security level at creation time. The apparently easiest choice from the user's viewpoint would have been to protect the information at the highest level until he completed the message and then have him assign the proper classification after reviewing the entire message. But the security model requires that when text is downgraded, it must be reviewed by the user so as to prevent malicious or inadvertent downgrading by the trusted process--a time-consuming process. Thus, the system required the user to assign the classification at message creation time. None of the users found this to be a problem. It was, of course, a nuisance to go through the time-consuming downgrading if a user found that his initial estimate of the classification was too high.

2.5.4 Capability to Reply at Different Level

One of the preliminary security designs, see [15], was based on a strict implementation of the *-property that disallowed the use of any trusted processes and thus did not allow downgrading within the system of any file. One of the consequences of this design was that a user could not use the automatic reply feature if the reply was to be at a lower security level than the original message. (The reply feature automatically fills in the ACTION and INFO addressees, precedence, subject, references, etc.) In early discussions with the users, it was clear that this was unacceptable. This resulted in a change to the security model that included the trusted process that violated the *-property under controlled conditions. The redesigned security model required that the user assign a classification level to his reply at the time of the reply.

2.5.5 Required Confirmations of Trusted Process Writedowns

The security of the system depended on the security kernel to control all writedowns (violations of the *-property) of classified data. Without this control, any program in a system such as this one could change the classification of, say, TOP SECRET information to UNCLASSIFIED and transmit it out of the system. Typically, programs like SIGMA contain on the order of half a million program instructions. It is impossible to verify the correct operation of a program that large. It is enormously difficult even to make a convincing argument that none of the code will downgrade classified information. (The problem of verifying the proper operation of a very large program was the motivation for the development of the security kernel.) The requirement for the user to confirm each writedown ensures that information

will not be downgraded without the user's knowledge. Further, it restricts the amount of information a maliciously-written trusted program could downgrade even if the user does not completely understand the security model. As stated earlier, most of the users did not fully understand the need for the confirmations and, thus, considered them an annoyance.

2.5.6 Review of Text for Downgrading

In any secure system, there will be a need for downgrading information. The amount of information that must be downgraded will depend on the granularity of the security controls. For instance, if the security is maintained at the file level, then a downgrade would occur whenever a, say, CONFIDENTIAL message is removed from a SECRET file. A downgrade is not necessary, however, if the kernel recognizes the security levels of both the file and the messages within the file. As the kernel maintains the security of smaller and smaller units (e.g., subject lines and individual paragraphs), then the convenience to the user increases (he doesn't have to downgrade an unclassified paragraph extracted from a SECRET message) and the overhead of the security controls increases. The AUTODIN system maintains security controls at the message level; thus, in SIGMA all parts of a received message were protected at the level of the message.

In the experiment, users were required to verify that text pulled out of a message to be downgraded contained no information at a security level higher than it should. Only a few users objected to this requirement.

2.5.7 Message Release

Ultimately the only way that mislabeled information could be sent out of SIGMA was through an outgoing message. Therefore, the release function was considered to be a part of the security controls; it and the comeback copy were the final security checks in the system.

2.6 Summary

An acceptable user interface can be developed based on the security kernel concept. Based on observations of system use and interviews with users, the restrictions on the user imposed by the security controls were tolerable and did not detract from the usefulness and convenience of the message system. Although the SIGMA implementation for the experiment did not utilize a security kernel to enforce the controls, it did interact with the users as if it did utilize a kernel.

A future interactive message processing system supported by a modified security kernel could dramatically increase the confidence in the security of message handling without placing undue restraints on the users' acceptance of the system.

SECTION 3
ENVIRONMENTAL FACTORS

3.1 Introduction

This section presents a summary of the performance and reliability of the MME System, a discussion of experience gained with the interface to the Local Digital Message Exchange (LDMX), as well as other environmental considerations.

3.2 Performance

Performance is a measure of a system's efficiency in responding to a user request. For example, a user may request a display of a file of messages awaiting action (DISPLAY FILE PENDING). Once the user has executed and confirmed this request, the system will collect the file, provide a display of a portion of the file on the user's screen, and allow the user to enter another instruction. The length of time required for the system to respond to the user's request is a measure of system response. Performance tends to be influenced by the number and complexity of the user requests being made over a period of time. A small number of users making complex requests may experience a slower response than a larger number of users executing simpler tasks.

MME users were provided with a measure of system performance in the form of a "Load Average" which appeared on their terminal screens. This load average was computed by the system based on the total number of users and the amount of system resources they were using. In some cases, the load average did not reflect all activity on the system (archive operations conducted by the system operator were not reflected, for example). Thus a low load average might have been displayed at the same time the user experienced a slow system response, but, in general, it was a good indication of the response a user could expect from the sytem.

3.2.1 Early Performance Measurement

During the February 1977 selection process, it was recognized that the performance of SIGMA was inadequate for the size of the task envisioned at CINCPAC. During these tests, SIGMA had been able to support only one or two simultaneous users with adequate response times. During the early phase of the experiment on site, users reported considerable dissatisfaction with the performance of the system for the limited number of terminals initially installed (less than 10). Lack of performance remained an impediment and prevented the installation of additional terminals until a significant hardware change was made in October 1978.

Several performance tests were conducted during the early part of the experiment. These tests used scenarios which represented typical system use by a varying number of users, from 1 to 20. Since no more than 12 users were ever simultaneously supported successfully during this period, a simulated load executing in conjunction with real users was provided through computer software. In January 1978 tests were run on a 512K KA processor under SIGMA

release 1.71. Five users were able to saturate the processor memory in that test. This saturation was evidenced by excessive operating system scheduling delays and page traps. Equally significant was the fact that CPU IDLE time was reduced to only 2%. While this may have been attributed in part to excessive use of the processor by the operating system, it was deemed to be an indicator of potential processor limitations as well.

Based on the collected performance data, changes were made to both software and hardware during the experiment to improve the performance of the system. Bottlenecks in the processing resources were identified and assessed for possible hardware and software modification. The main memory was increased to 768K words in April 1978. Then a KL processor, a total of a million words of memory, and increased disk capacity were installed in October 1978.

Software modifications were also made to improve performance as well as to enhance overall system capabilities. The interface between the operating system (TENEX) and the application program (SIGMA) was examined for possible sources of inefficiency, and changes to that interface were implemented.

3.2.2 SIGMA Maintenance and Modification

This section discusses the process by which changes to SIGMA were made. The MME staff was in frequent contact with system users. One result of this interaction was a documented series of "User Comments." For example, during a training session, a user mentioned that it "would be useful if the system would let me know when a Flash precedence message arrived." The comment was recorded along with the name and office of the commentor, a note about the circumstances under which the comment was made, and a notation of the general area of the MME system about which the comment was made. In this case it was the message handling subsystem.

Documented User Comments and other informal recommendations for change were consolidated, amplified, and documented in a Desired SIGMA Enhancement List (DSEL). The user comment referred to above was incorporated in the list by an item reading: "The system should alert the user when incoming messages are received, that have subjects of interest to the user or are of high precedence."

Items from the Desired SIGMA Enhancement List were prioritized and developed into specific requirements for system change. A Configuration Control Board (CCB) established priorities and approved development and implementation of any charge. The vehicle for documenting a proposed change was the Functional Change Request (FCR). The FCR was written by representatives of the user and development groups and reviewed and approved by the CCB before development of a software change was initiated. The FCR addressed the following aspects of the functional change:

(a) Description of the functional change

(b) Reason for change

(c) Description of design change implied by the functional change

(d) Impact of the proposed change on data collection, documentation, human factors, testing, operations, performance, security, and training

(e) Alternate changes or designs

(f) Recommendations

(g) Disposition

Following the example of the user request for an alert, an FCR to incorporate an ALERT function in the system was approved by the MME CCB and implemented in Release 2.2 of the SIGMA software. This feature provided user controlled alerts based on various message header criteria.

Development and implementation of changes in the system software were also controlled by the MME Configuration Control Board. A major modification of the system (change in the daemon structure for example) would require a new SIGMA "Release." Modification of current system capabilities or correction of a system anomaly would be accomplished in a "mini-release."

Development of releases and mini-releases were done at ISI. After testing at ISI, a magnetic tape containing the change was made and sent to the MME site. On site, the change was incorporated in a test version of the operating system and provisions were made for a test team to use the new version of the software. Testing included a review of previously available functions—to ensure upward compatibility of the new release—and an examination of the new features of the release—to verify that they were present in the release and to verify training and system documentation. The operating system was "cut-over" to the new release after results of the testing process were evaluated by the CCB. A summary of the major and mini releases is found in Table 2.

3.2.3 Subsequent Performance Measurements

After the system began to be used in a limited manner by the J3 staff, a series of benchmark tests was performed using two versions of a similar scenario. These tests were run after the installation of each software release and each hardware upgrade. Test conditions for these benchmark tests provided a similar setting for the entire series of tests. All regular use of the system would be shut off, the LDMX link would be halted, and specific data-collection utilities would be started up. A typical series of benchmark tests would involve first five, then ten, and finally fifteen individuals with specific scenarios exercising the system. The results of the benchmark tests provided a comparison among the various software releases in terms of performance and provided clues for future improvements. These results are shown in Table 3.

TABLE 2. Summary of SIGMA Release Features

Release 2.0 was installed in July 1978 and contained the following features:

ROUTE COMMAND Provided for routing one or more messages to one or more offices/files using only one command. (Based on a Desired SIGMA Enhancement)

ON-SITE TEST A performance measurement tool.

MESSAGE TURNAROUND Provided a turnaround file for messages received in error from the LDMX. (Based on a Desired SIGMA Enhancement)

Release 2.02 was installed in August 1978 and contained the following features:

EARLY ARCHIVE Provided early archive for FBIS and weather messages. (Based on a Desired SIGMA Enhancement)

PRINTER OPERATION Provided a print module that did not reformat text. (Based on a Functional Change Request)

Release 2.2 was installed in January 1979 and contained the following features:

ALERTS Provided user controlled alerts based on various message criteria. (Based on a Functional Change Request)

READDRESSALS Corrected format to allow for LDMX automatic processing of readdressal requests. (Based on a Functional Change Request)

ACTION/PERSONAL FILES Allowed access to personal files when logged on as an office. (Based on a Functional Change Request)

EDITOR/VT Provided faster system response to individual user jobs. (Based on a Functional Change Request)

RELEASE TO LDMX Notified operator upon message transmission. (Based on a Functional Change Request)

EFTO Provided capability to create and transmit EFTO messages. (Based on a Functional Change Request)

Release 2.21 was installed in January 1979 and contained no new features.

TABLE 2. Summary of SIGMA Release Features (continued)

Release 2.22 was installed in February 1979 and contained the following features:

TEXT FORMATTING	Provided capability to selectively reformat text. (Based on a Functional Change Request)
CITATION DAEMON BACKUP	Provided for a backup citation daemon in the event that the primary daemon aborted.

Release 2.23 was installed in April 1979 and contained the following features:

FIND TOP/FIND BOTTOM	Allowed system to find top and bottom of a file. (Based on a Desired SIGMA Enhancement)
KEYWORD DISPLAY	Provided capability to display keywords associated with a file. (Based on a Desired SIGMA Enhancement)
EXECUTOR IN CHOP FIELD	Allowed system to automatically insert the identified name in the chop field when chopping a memo/message. (Based on a Desired SIGMA Enhancement)
SSO DELETED MESSAGES	Marked message citations DELETED BY SSO for messages deleted due to security implications.
ADDRESS DOMAIN COMPACTION	Allowed more than one addressee per address line on memos. (Based on a Desired SIGMA Enhancement)
AUTODIN 63 CHARACTERS	Reformatted AUTODIN template to allow for a maximum of 63 characters per line of text. (Based on a Functional Change Request)
READDRESSAL DTG	Used DTG of original message versus subsequent retransmitted DTGs. (Based on a Functional Change Request)
SIGMA EXEC	Allowed use of SIGMA EXEC as a diagnostic tool to study jobs that were abnormally terminated.
BACKCOPY CID	Placed appropriate CIDs on backcopy citations. (Based on a Desired SIGMA Enhancement)

Release 2.3 was installed in June 1979 and contained the following features:

COMMENTS ON FILES	Provided capability to comment on file entries. (Based on a Desired SIGMA Enhancement)

TABLE 2. Summary of SIGMA Release Features (continued)

MEMO FORMATS	Provided memo formats compatible with CINCPAC format. (Based on a Desired SIGMA Enhancement)
TEXT HIGHLIGHTING	Provided capability to selectively highlight message text. (Based on a Desired SIGMA Enhancement)
READBOARD AIDS	Provided capability to empty files without opening them, sort files by DTG, and to highlight individual file entries. (Based on a Desired SIGMA Enhancement)
COMMENT LOCATION	Provided capability for operator to check queue status for various system jobs. (Based on a Desired SIGMA Enhancement)

Release 2.3.1 was installed in July 1979 and contained the following feature:

LIMITED ACCESS	Allowed for controlled distribution and access of sensitive messages. (Based on a Functional Change Request)

TABLE 3. Summary of Benchmark Tests on SIGMA Release 1.75 and 2.0 with 1 to 12 Users

Date of Test	6/13/78	6/13/78	6/14/78	6/13/78	6/13/78	6/14/78	6/14/78	6/14/78	
Number of Users	8	8	8	12	12	12	1	4	
Amount of Core	512K*	768K	768K	512K	768K	768K	768K	768K	
SIGMA Release	1.75	1.75	2.0	1.75	1.75	2.0	2.0	2.0	
Elapsed User Time	32	32	26	64	52	46	7	15	(min)
Elapsed Daemon Time	37	37	35	74	60	53	13	21	(min)
Normalized User CPU	107.0	106.5	89.4	133.9	115.7	97.4	85.2	83.6	(sec)
Normalized Daemon CPU	93.0	91.0	80.5	99.0	88.9	74.4	147.0	103.0	(sec)
Normalized Total CPU	314.6	306.0	259.0	420.0	339.5	282.8	436.0	277.0	(sec)
Maximum Paging Rate**	69.4	63.5	60.0	107.0	83.5	77.0	23.7	39.0	(pgs)
5 Command Average*** (First User)	51.7	65.8	34.2	148.2	99.2	91.1	3.4	8.4	(sec)
5 Command Average*** (Second User-- Stop Watch Time)	38.6	75.0	40.0	137.0	102.5	94.6	----	----	(sec)
Aver. User Real Time (Logon to Logoff)	25.0	25.0	21.0	56.0	44.0	36.0	7.0	11.0	(min)

* All tests conducted on KA System.

** Data expressed in pages per second.

*** Functions observed were VIEW NEXT and DISPLAY NEXT.

3.2.4 Observations and Conclusions

System responsiveness was considered a critical issue from the outset of the experiment. However, the system modifications necessary to improve responsiveness were more extensive than originally envisioned. Software, hardware, and operational concepts all required examination and modification in order to bring the system up to a useful level of performance for twenty users.

It was noted that experienced users tended to be more forgiving of slow response time than did new users. Since the system was "new" to all users at the beginning of the experiment, most users expressed dissatisfaction with its performance at that time. Often, however, their dissatisfaction might have been more appropriately addressed to some other aspect of system operation such as terminal malfunction or user procedures.

System performance influenced user procedures. Changes were made in the style of use which could be attributed, in part, to improving system performance. For example, at the beginning of the experiment, all message traffic was routed to each participating office by J301. A change in the SIGMA system provided all users direct access to all traffic. Users built complex filters to scan this file for individual messages of interest, thus bypassing the J301 router.

Ultimately the changes to hardware, software, and procedures produced a system which adequately supported twenty users simultaneously. The processor hardware necessary to provide this support was far in excess of that hypothesized before the experiment began. The flexibility and features offered by the SIGMA software system architecture contributed in large part to this need for expanded processing resources. The architecture was, in turn, fundamentally a result of the open-ended requirements placed on SIGMA by the experimental environment. Further, because of the imposition of a particular operating system (TENEX), the developers were not free to choose or design an operating system that was a better match for SIGMA. As it turned out, many of the overload problems were caused by a mismatch between SIGMA and TENEX. TENEX was simply not designed to support a program like SIGMA. See volume V [9] for a more detailed analysis of the SIGMA/TENEX interface.

3.3 Reliability/Availability

This section discusses the reliability/availability of the MME System as measured by its ability to accept and complete user-initiated tasks. The section also discusses problems encountered, which, from time-to-time, reduced the system availability below an acceptable level.

3.3.1 Summary of Weekly Availability Data

Figure 4 provides a summary of system availability during the Full Experimental Use period of the MME. The Quick Look Report [17] and Mid-Experiment Report [22] provide similar data for previous periods of the experiment. This availability summary recorded the periods of time on a weekly basis in which the system was and was not available for J3 use. During

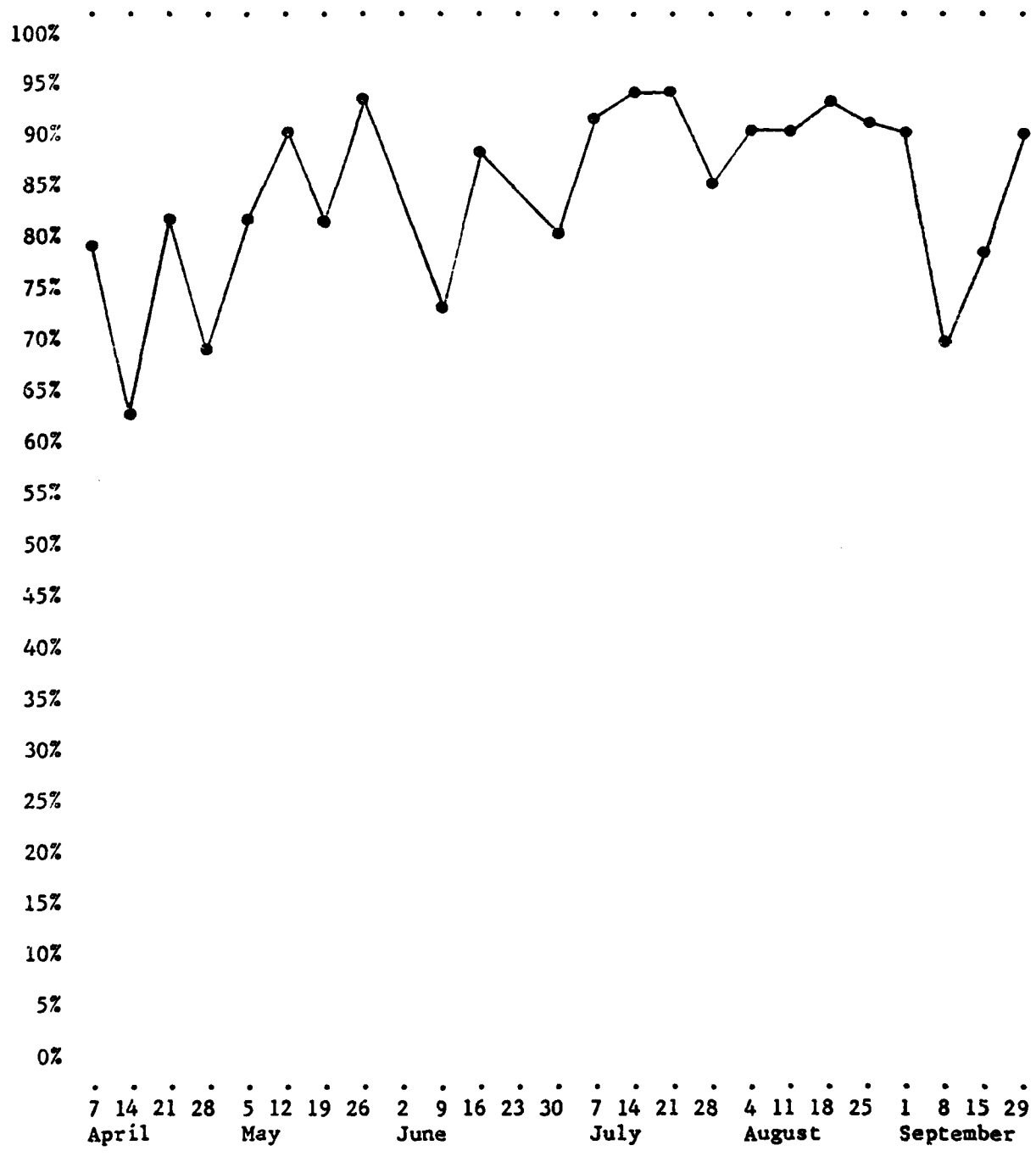


FIGURE 4. System Availability During Full Experiment Use - 1979

the experiment it was noted that while the system may have been available for use by J3, certain individual users may have been denied access due to problems encountered with their terminals, interconnection with the computer, or a software malfunction. To identify, measure, and evaluate these individual user problems, the term "Abnormal Termination" was introduced to denote a situation in which a user's job was halted by any means except a user logoff. In October-November 1978, 15% of all jobs initiated by users were abnormally terminated.

3.3.2 Extended Outage Discussion

On 5 April 1978, disk memory problems which had been causing frequent system halts, caused complete destruction of the file system. Consequently, the system was deliberately kept unavailable while attempts were made to identify and correct the disk problem.

In December 1978, many problems were encountered with the disk memory system. The disk drive and backup disk controller were down for an extended period and user files were damaged. The overall system availability for December was 86.8% compared with 98.4% and 97.4% for October and November. The disk problems continued intermittently through February. In March 1979, a malfunctioning filter on the main power line was removed. This, along with corrective measures to the electromechanical portions of the disk subsystem, temporarily restored the MME system stability. The system availability increased from 92.9% in January and 83% in February to 96.8% in March. A new disk subsystem was installed in April. Throughout the period, availability to the user remained at 87% of the 24 hour per day goal. As Figure 4 shows, the availability tended to be sharply sloped with good and bad weeks.

The lack of reliability of the MME system was a major complaint of the CINCPAC staff users. It had an impact on their perception of the MME system in particular and automated message handling in general.

An early indication of the importance of the role of reliability in the users' views of the system came in their responses to questionnaires in surveys conducted prior to the publication of the Quick Look Report [17] and the Mid-Experiment Report [22].

In response to the first questionnaire, users:

- identified reliability as a major problem and foresaw some limit to system usefulness as a result; and
- observed that poor reliability during a critical time might render the system useless just when it was needed most.

In response to the second questionnaire, users said:

- the lack of system stability had a deleterious effect on the training of the users;

unless users were confident that the MME was not going to fail repeatedly there would continue to be resistance to using it; and

"the system will still do you in if you don't take time to do a FINISH every once in awhile to protect work."

(The latter recommendation is interesting in that users were beginning to learn the protection features available in the SIGMA System. FINISH preserved a copy of work in progress so that changes to the document up to the point of the FINISH would not be destroyed. FINISH also closed the object; this was irritating to a user because he then had to re-DISPLAY in order to open the object for edit. A simple SAVE function for a partially complete message was needed. Such a function was available for saving text objects but not entire messages.)

During the period of operation covered by the Mid-Experiment Report, the major complaints were the lack of reliability, the insufficient number of terminals and the slowness of the SIGMA System for reading and sorting messages. These complaints were factors in reaching some of the more general conclusions concerning future message handling systems that were reported in [22].

3.3.3 Observations and Conclusions

The user was the ultimate determinant of system performance. If the system took a long time to perform tasks that users perceived as "hard," they were rather tolerant. They were briefly intolerant of extensive delays in the performance of "easy" tasks. Yet, users could and did learn to use a slow system--in some cases they altered their method of operations. For example, users learned to short-circuit the distribution problem by going directly to the date file, a file of messages with a common date of origin; this file was available to all users. However, they could not use a system that was unavailable. They could and did learn to protect their work from the potential situation that the system might fail during use through periodic executions of the SAVE and FINISH commands.

Users demand, however, that an interactive system that they depend on to accomplish their daily tasks and to resolve problems in a crisis must be nearly 100% available. Although they may not notice downtime in a system that they access via paper (such as the LDMX), they are acutely aware of the downtime in a system that is accessed via a terminal in their offices. In order for an Automated Message Handling System (AMHS) to be reliable from the users' perception, its software must be thoroughly tested and debugged, its hardware must be reliable and redundant, and the system must be housed in a suitable physical environment.

Availability is, in fact, a more difficult problem to deal with than performance. The problems encountered in the area of availability required a more system-wide (external to the computer) approach to resolve than did those associated with performance. While improvements to SIGMA tended to provide a fairly constant increase in the level of performance, the system as a whole tended to have catastrophic failures on a regular basis.

3.4 Interface to AUTODIN/LDMX

The Automated Digital Integrated Network (AUTODIN) provides long haul trunk telecommunication facilities for military message handling. Use of these facilities requires special interface units which receive and transmit traffic in a format used by AUTODIN. At Camp Smith, a Local Digital Message Exchange (LDMX) is used for this interface. The LDMX provides initial routing of incoming traffic to the CINCPAC Directorate level, special handling of high precedence incoming traffic, and message file and accounting functions.

3.4.1 CINCPAC LDMX Operation

Electronic delivery ports are used to deliver traffic to various devices such as printers or user-oriented systems such as the MME. Low precedence traffic that is SECRET or below and consists of a single section is directed to a line printer with initial internal distribution annotated. A printing press is then used to create the required number of copies for distribution. These copies are then pigeon-holed for pickup by directorate personnel. TOP SECRET traffic is routed to a special output device. Electronic duplication of the TS message is closely controlled. High precedence traffic is directed to a special electronic line within the CINCPAC Command Center, regardless of classification, in addition to the routing dictated by its classification. Messages of more than one section are annotated and delivered to the line printer but are withheld from printing until all sections have been received. Frequently, sections of messages will be received out of order.

Released outgoing messages are processed for AUTODIN transmission by the LDMX. An Optical Character Reader is used to scan a specially prepared paper copy of the released message. The OCR provides an electronic translation of the message on which the LDMX acts. Addressees of outgoing messages are verified for correct format, routing indicators are applied, and a Date Time Group is assigned. Comeback copies of outgoing messages are also produced by the LDMX. Long messages are broken into several sections for transmission.

Readdressals are retransmissions of an incoming message to outside addressees. The process of readdressing a message is initiated by a drafter completing a memorandum form to the telecommunications center which requests that a message be readdressed to other activities. This form is then released and forwarded to the telecommunications center. At CINCPAC, the memorandum form was read by the optical character reader, the message electronically "found" in the LDMX files, a new header (addressees and Date Time Group) applied, and the message transmitted to the new addressees.

Date Time Group files of recent incoming and outgoing messages (15 days) are retained on-line and a magnetic tape interface is provided to archive and restore older messages. These files are used to respond to user requests for copies of messages after initial distribution and in the readdressal of incoming messages.

Problems may arise in the telecommunication system which require retransmission of an outgoing message. A "service" message may be created within the telecommunication system which uses a form of communicator's

shorthand to indicate the reason for the retransmission request and in most cases refers to the serviced message by channel sequence number or other communication system generated identifier. The LDMX may automatically respond to such a request or a service clerk in the originating communication center may initiate a response to the service message. A response to a service message typically includes a copy of the original message and an annotation that the new message is a duplicate of the previous message. In some cases, the drafter must be contacted to verify material to be transmitted. In most cases, the message is delayed in its delivery to an addressee until the service message is resolved.

3.4.2 Interface to MME

The electronic link between the LDMX and the MME System consisted of two assigned LDMX Logical Reference Number (LRN) ports, a wire connection, and software. This link provided for transmission and reception of AUTODIN messages and communication protocol between the two systems. Incoming messages to the MME were provided after initial internal distribution decisions were made in the LDMX and generally duplicated the paper copy distribution of messages to J3 components at classification levels below TOP SECRET. Outgoing messages were transmitted via a second LRN to the LDMX. The LDMX addressee verification and routing indicator processing were used by the MME on outgoing traffic. Readdressal processing consisted of the transmission of an electronic version of the readdressal request to the LDMX. Action by the LDMX on the readdressal was similar to that provided for readdressal requests entered by the OCR. Separate files of incoming and outgoing messages were maintained by the LDMX and the MME Systems.

The structure of the LDMX offered several points at which incoming traffic could be electronically delivered to a user-oriented system. For example, the Command Center received all incoming high precedence traffic addressed to CINCPAC regardless of classification or LDMX internal routing decision. The MME received traffic after precedence, classification, and initial routing decisions were made in the LDMX. TOP SECRET traffic was delivered exclusively to the TS Printer. Changes to the LDMX to allow duplicate delivery of TS traffic to the Printer and MME were beyond the scope of the experiment. Traffic available in the experiment was therefore limited to that classified SECRET and below.

In the manual system, a typed copy of an outgoing message and information about its releaser and drafter including name and phone number are hand delivered to the telecommunications center. The message is scanned by an optical character reader prior to its acceptance by telecommunications center personnel for transmission. Information concerning the releaser and drafter are stored in the LDMX file along with the text of the message. In the automated system as represented by the MME, an electronic version of the message was sent to a processing component of the LDMX. This process bypassed the verification steps afforded by the OCR. The electronic version, in the case of the MME, did not include identification of the drafter or releaser of the message. Therefore, it was difficult to contact the originator of a specific message. The MME operator did not have immediate access to outgoing messages and could not help identify the originator. The impasse was usually

resolved by the System Control Officer contacting various release points to track down the drafter.

The MME System was used to generate readdressal requests. The requests were electronically handled by the LDMX. When errors were encountered in the handling of MME readdressal requests, the telecommunications center service position was notified. The LDMX archive file contained 15 days of back traffic. The MME System was capable of producing messages several months old. At times, users wanted to readdress messages older than 15 days. Because the LDMX file did not contain the message, it could not satisfy the readdressal request and notified the MME system using a service message.

3.4.3 Summary and Conclusions

Two problem areas stood out as candidates for consideration by future builders of AMHS systems.

First is the incompatibility between the message service and telecommunications systems in light of user requirements. The MME used an electronic "memo" to the LDMX in readdressing messages. The MME user would search a datefile for the message he wished to readdress, fill out the appropriate information in a system provided form and release the "memo" to the LDMX. A major problem arose if the message were no longer on-line at the LDMX. If this case occurred, the LDMX would alert a service position for human intervention. Human intervention required settlement of jurisdictional prerogatives (who is responsible for resolution of the problem: the LDMX to locate the message in its archive—or the drafter/releaser of the request for a retransmission). The end result of the process was at least a delay and at worst a non-delivery. The second large-scale problem was in the area of service messages. Service messages are communicators' shorthand messages used to account for other messages. For example, if a message is received with an addressee that is unknown, the communicator might send a service message to the message originator requesting a retransmission of the message. The problem with service messages in terms of the MME was that the user (or the MME operator) (1) usually could not understand the shorthand used in the service message, (2) frequently could not identify the message to which the service message referred, and (3) could not reintroduce the same message under the same Date Time Group to satisfy the request. Experience also showed that service messages on MME outgoing messages wound up in jurisdictional discussions between the telecommunications center and the MME Staff. About 30% of all outgoing MME messages required service. Both of these problems illustrate the need to consider the development of an AMHS with the total telecommunications process in mind.

SECTION 4
USER SUPPORT

4.1 Introduction

A major objective of the designers of the Military Message Experiment was to disrupt CINCPAC J3 operations as little as possible, consistent with achieving the goals of the experiment. It was vital, of course, that J3's ability to do its job relating to military operations in the Pacific not be impaired. This meant not only not taking away needed capabilities during operations, but also not distracting people from their jobs. In order to address this concern, a three-pronged approach was taken. First, a comprehensive training program was developed, involving instruction by both man and machine. Second, an on-site staff was placed at CINCPAC to respond quickly to user problems. Finally, SIGMA was designed with flexibility in mind so that it could be modified in response to user requests for change. In the following paragraphs the details of MME user support are provided.

4.2 Training

A training director was provided as part of the project staff, rather than using someone from the user community, so that he could devote full time to the experiment. (For a complete description of the training program, see [11].) By working closely with other project personnel, he achieved a level of expertise that might not have been possible for a J3 staff member with other duties. The trainer was also responsible for responding to user questions throughout the day, and stayed on-site for the duration of the experiment. An important feature of user training, designed to reduce operational impact on the user, was the decision to make heavy use of an on-line tutor rather than formal classroom training. One of the perceived advantages of on-line lessons was that they would avoid the air of pedagogy present in a classroom, which middle and senior grade officers might have found irksome. With an on-line tutor, users could take lessons in their own workspace at the time that was convenient to them. This meant that the office need not be understaffed when people were excused to go to class; if something came up requiring the attention of the lesson-taker, he could leave the terminal, attend to office business, and then resume the lesson at the point he left it. Another advantage of on-line lessons was that a user could proceed at his own pace. If he felt the need to retake a lesson, he could do so without embarrassment. Conversely, if he was learning the material quickly, he could proceed to advanced lessons without having to wait for fellow class members to reach his level.

The MME training program had four main components--an introductory lecture, on-line lessons and exercises, printed documentation, and individual training sessions. In addition to these components, on-line aids provided by the system helped users learn specifics of system use, and special documentation was provided on-site as the need arose.

The purpose of the introductory lecture was to introduce new and potential users to the system in a manner that would explain the objectives of the experiment to them and motivate them to use it. The lecture was intended to overcome any tendency to think the automated system was just something else to learn--a complex stumbling block for users to surmount to get their job done. The lecture was not intended to train users, but to prepare them for training--to bring them up to the level at which they would be able to log on and take lessons.

The on-line lessons were expository in nature and discussed aspects of commonly used instructions. Exercises allowed users to practice instructions that were being taught in the lessons in a tightly controlled environment, using messages and files especially designed for that purpose. Great care was taken to see that lesson takers could not accidentally damage operating files and messages while taking lessons.

Printed documentation had a role in training as well as serving as a reference source for operations. ISI published a Primer for the use of SIGMA, as well as a detailed Reference Manual. In addition to formally published material, printed handouts were distributed from time to time to some or all of the users.

Another aspect of the training program involved supplying users with individual training sessions when they required them. These sessions were either general in nature, dealing with all aspects of the system, or tailored to fit the needs of a particular user's job. In some cases, they consisted only of the trainer watching the user performing his message-handling duties and making occasional suggestions, but in others they involved some study of the office functions by the trainer, followed by distribution of handouts and follow-up sessions.

In addition to the training program just described, SIGMA provided its users two special terminal keys--labelled PROMPT and HELP--that they could use for support during operations. The PROMPT key responded by displaying in a special format all alternate forms of the instruction being typed or, if the instruction line was empty, all instructions legal in the given situation. The information was succinct--one line with the syntactical information, and one more line of explanatory material. The user could put the cursor on an instruction of interest and press PROMPT again to see a slightly more detailed explanation of each of the terms used in the syntactical definition. When he wished the screen to return to its pre-PROMPT state, he pressed the PROMPT key one more time. The HELP key made available to the user an on-line form of the Reference Manual. It provided him with a mechanism for switching the display from one topic to another (in effect, turning pages in the manual). By moving the cursor to certain locations on the display and pressing the HELP key, the user could turn to a selected topic, or return to a previous topic, or type in a new topic and turn to it. When he was finished browsing, he could return the screen to its regular display by pressing the CANCEL key.

During the course of the experiment, the type of training users received gradually changed. In the preliminary period, most information came from the experiment staff, especially the training director. During this period, when

SIGMA was neither as reliable nor as responsive as it was later, lesson-taking was more awkward, and on-the-job training was less rewarding. The users had to put more reliance on documentation, information from the experiment staff, and information from experiment liaison people within J3. Some statistics on lesson-taking during the preliminary period have been previously published [11].

As Limited Experimental Use (LEU) approached, one-on-one sessions were held with several of the users. In particular, from 10 May 1978 until 28 June 1978, the training director sat in on eleven J301 message routing sessions, for periods of time ranging anywhere from one to three hours. Since the routing of messages to their ultimate recipients was viewed as a critical step in the use of the system during LEU, it was particularly important that it got off to a good start. Three different people carried out the routing, and gradually each learned the instructions he needed well enough to do his job effectively.

As time passed, users were better able to learn from the system itself, by means of on-line lessons and on-the-job training, and by information given to them by other users. At the same time, there was a wider variety of written material available (for example, the User's Guide and various special handouts). In the last two months of the experiment, some of the new users who stood watches in the CINCPAC Command Center received virtually all their instruction by on-the-job training and by training by their peers, rather than from the experiment staff.

From November 1978 until June 1979, J3 issued a series of "MME Training Reports," usually at weekly intervals. These reports were circulated to all users of SIGMA by creating and distributing a message using SIGMA. They divided users into four categories: those who were trained, those who were partially trained, those who were marginally trained, and those who were untrained. Users were graded as untrained after they had received the introductory lecture but before they began to appear in the session transcripts (weekly summaries of SIGMA usage). After their names began to appear in the session transcripts, they were moved into the marginally trained category. Their further progress depended both on how frequently they used the system and on comparing the sorts of instructions they were issuing with those contained in the milestones established for their particular office. The decision on what category in which to place a particular user thus required much subjective judgment on the part of the J3 MME Training Coordinator, a Navy Chief Petty Officer who was a very experienced user.

Table 5 summarizes the training status of the users, as shown in the J3 reports, for a few selected weeks. It should be noted that some of the fluctuations in these figures can be accounted for by transfers into and out of the test group during the experiment, and other fluctuations may be due to changes in perceptions as to whether or not one or two small offices should be included in the test group.

It has already been noted that one of the principal training tools was expected to be the on-line lessons which formed a part of SIGMA. Table 5 provides some lesson-taking statistics. Whenever a user took a lesson, SIGMA

TABLE 5. User Training Proficiency
Entries are in percentages.

	Observation Period				
	Nov 78	Jan 79	Mar 79	May 79	June 79
Trained	25	38	61	88	91
Partially Trained	6	11	18	7	0
Marginally Trained	25	33	17	2	0
Untrained	44	18	4	3	9
Total Number of Users	100	109	103	107	99

TABLE 6. Lesson-Taking Summary

Lesson Number (N)	Number of Users Taking lessons 1 Through N	Number of Users Who Took Lesson N
12	11	11
11	1	12
10	2	14
9	3	17
8	4	21
7	8	29
6	5	34
5	15	49
4	14	63
3	19	82
2	18	100
1	16	116

automatically created a record in a session transcript file. Using these records, it was possible to keep track of the lesson-taking activities of 207 potential users. In some cases, a user might have taken a particular lesson more than once; the statistics in the table do not reflect this multiple usage. It can be seen, for example, that 19 people took exactly three of the lessons, while 82 people took three or more. From the data in the table, it is also clear that 44% of the user population (or 91) took no lesson at all. Further, for those who did take the lessons, most seemed to stop after four or five and did not go on to complete the entire set. Subsequent assessment by the on-site staff tended to show that those users who took a greater number of on-line lessons were more proficient in the use of SIGMA that those who took only a few lessons.

From the data collected during the MME, certain conclusions concerning training can be drawn. First, users generally preferred training in their office environment, in small groups, or even one-on-one. Large classroom situations and printed reference materials, while generally found useful, were not as well received as the on-the-job training. Further, use of the system itself for training (via PROMPT, HELP, or the on-line lessons) was, in the main, negatively received. The data, however, could support many different conclusions. It might have been that the computer instruction was poorly designed and therefore was not viewed positively (user interviews support this conclusion), or it might be that the process of learning at the computer was not a positive experience for the J3 users. It is also interesting to note that while those who took more on-line lessons were deemed to be better trained than others, it is possible that only those who were pre-disposed to learning the automated system took the lessons and would have been more proficient under any circumstances.

4.3 On-Site Staff

An on-site staff was provided by government and contractor organizations participating in the experiment. In general, the staff operated in three functional areas: operation and maintenance of the system hardware and software, system user training and liaison, and experiment evaluation and coordination.

Operation and maintenance of the MME system included functions related to monitoring system processing and communications functions, file space maintenance, hardware preventive and corrective maintenance, software maintenance, and file system restoration in the event of system failure. The following personnel were involved in these functions.

The System Control Officer (SCO) was responsible for the execution of system maintenance and testing schedules and provided guidance and direction to system operation and maintenance personnel through the Facility Manager. The SCO was also responsible for maintaining the proper operation of the communication elements of the system which included the link with the Camp Smith Telecommunication Center, and two links to user organizations located remotely from the central processing facility in other buildings at Camp Smith. The SCO was responsible for the application of resources to effect timely restoration of services after system outages. The System Control

Officer was a Navy Chief Warrant Officer with extensive experience in message handling and technical control center operations.

The Facility Manager was responsible for the proper operation of system hardware. The system operators and software and hardware maintenance personnel reported to the Facility Manager. Personnel filling this position had experience in management of computer centers and customer relations. The Facility Manager was responsible for the following:

(a) ensuring maximum availability of system hardware for operational use;

(b) reviewing and approving system operating procedures;

(c) maintaining system hardware and software;

(d) coordinating operator training;

(e) developing status reports and analyses of computer system malfunctions; and

(f) developing necessary documentation for the proper operation of the computer system.

The Operations Supervisor was responsible for:

(a) defining and reviewing operator assignments and tasks;

(b) promulgating operational procedures;

(c) monitoring system availability on a continuous basis;

(d) reporting outages to the SCO and Facility Manager;

(e) maintaining MME System software logs; and

(f) providing assistance to users as required.

System Operators monitored system processing and communication functions on a continuous basis, made periodic backup copies of the file system and archived messages to magnetic tape on a periodic basis. Operators also responded to user requests for restoration of a terminal or printer to service when the system unexpectedly terminated the user job.

Software Maintenance Technicians made all password and account changes, assisted in installation and testing of new versions of the software, and restored system files in the event of a crash. Hardware Maintenance Technicians performed corrective and preventive maintenance, assisted in resolving telecommunication equipment problems, and installed, checked, and maintained user terminals and printers.

Interaction with system users was essentially a four-phase cycle, which included:

(a) introduction of the user to the basic capabilities of the system through training;

(b) observation of system use to identify useful system features, user preferences, and impediments to effective system use;

(c) definition of requirements for system or procedural modification through discussion with users and developers; and

(d) introduction of system or procedural modification.

Several people were involved in these activities. The Training Director was responsible for the interaction of users with the MME System. This included:

(a) maintaining cognizance of MME data collection activities;

(b) promulgating the MME System user procedures;

(c) maintaining open communications with the user community and developers; and

(d) providing user training.

The User Liaison Coordinator reported to the Training Director and was responsible for the following:

(a) collecting and maintaining user comments and initiation of Functional Change Requests (FCR) when appropriate;

(b) coordinating response to user comments;

(c) developing scenarios for directed MME System use;

(d) coordinating MME System demonstrations; and

(e) coordinating System Modification Testing.

The Data Collection Coordinator also reported to the Training Director and was responsible for:

(a) coordinating Session Transcript collection and promulgation;

(b) developing and maintaining on-site records of the MME System use; and

(c) collecting and correlating subjective data on the MME System utility.

Evaluation of the system, the operational environment, and the overall experiment objectives required coordination of staff activities to ensure maximum availability of the system, non-interference in the work of the CINCPAC staff, and that the objectives of the experiment were being met through the activities of the staff.

The On-Site Experiment Director was responsible for on-site experiment control and for implementation of elements of the MME Test Plan [29]. He maintained informal day-to-day liaison with the CINCPAC Project Manager and other memebers of the CINCPAC staff and provided the On-Site Coordinator with status information concerning the operation of the system. He also assisted the On-Site Coordinator in identifying and resolving problems requiring action by MME evaluators. Periods required for exclusive use of the system for planned maintenance, testing and installation of new hardware and software were scheduled by the On-Site Experiment Director, and he coordinated the on-line testing of various system features by MME staff members.

The On-Site Coordinator was responsible for the overall coordination of the experiment and was the on-site representative for DARPA. The On-Site Evaluation Committee Member was responsible for collecting information, observing the users, and recommending changes to enhance the utility of the experiment results.

All of the on-site staff just described performed duties solely related to the support of the MME. The size of the staff, nineteen in all, reflected the need to cause as little disruption as possible to the CINCPAC operations, to provide responsive support to the users, and to collect the data necesary for the proper evaluation of the MME.

4.4 System Evolution

The development of a stable, useful system to support the experiment required several changes in hardware and software during the operational phases of the experiment. Performance, reliability, and utility in the CINCPAC environment were critical issues throughout the experiment. System response time was initially unacceptable and the number of users that could be supported was limited until modifications related to performance were developed and installed. The consistent availability of the system was impaired by lack of useful redundant hardware, cumbersome file system restoration techniques and lack of a reliable electrical power source. Changes in hardware and software were made during the operational phases of the experiment to enhance the availability of the system. Functional changes in the system also evolved as users became familiar with the potential capabilities of the system and the telecommunications handling system in effect at CINCPAC became better understood by the development community.

Although SIGMA had been designed in response to a specific set of requirements developed in conjunction with members of the CINCPAC staff, experience using the system led the users to request additional capabilities during the course of the experiment. Although some of these requests could not be satisfied due to constraints of the SIGMA design or of the limited time available, many user requests were satisfied. Table 7 briefly describes the capabilities asked for in the form of Functional Change Requests (FCRs). One of the functions implemented, FCR #27, was a set of readboard creation aids. These were "file and sort," "move and sort," "empty file," "sort file," and "highlight." With the exception of highlight, these functions were designed to let the user accomplish several actions with a single instruction. (The "route" instruction, implemented before the system was opened to general use

TABLE 7. Requested SIGMA Capabilities

FCR #	Title	FCR #	Title
1	Route Command	21	Multiple HERE
2	On-Site Test	22	Find Top/Bottom
3	SIGMA Logon	23	Fast Folder Update
4	Message Turnaround	24	Memo Formats
5	Subject Algorithm	25	Text Highlighting
6	Early Archive	26	Limited Access
7	Printer Operation	27	Readboard Aids
8	System Status	28	Keyword Display
9	Alerts	29	Comment Location
10	Printer Notify	30	Executor in Chop Field
11	Readdressals	—	Highlighting Subject in File Entries
12	Action/Personal Files	—	SSO Deleted Messages
13	Editor/VT	—	Queue Status for CCP
14	Discretionary Access	—	Citation Daemon Backup
15	Text Formatting	—	Address List Domain Compaction
16	Release to LDMX	—	AUTODIN 63 Character Lines
17	EFTO	—	Readdressal DTG
18	Comments on Files	—	SIGMA Exec
19	Corrections to Reply	—	Backcopy CID
20	Tab	—	SIGMA Documentation

at CINCPAC, was also designed at the request of the users.) The readdress instruction and the alert list capabilities are other examples of features the users requested and received.

Any system that has not received operational use, no matter how well researched, will need additions or changes to tailor it to the user community. It is therefore important that the staff which supports the system be organized to accept and discuss changes with the users. It is also important that the system be designed so that changes can be made without major disruptions to the users. During the MME, several procedures were implemented to ease this process. Meetings were held with representatives from the J3 staff to discuss requests for changes or new functions. When this combination of users and support staff had agreed on the desired feature, it was presented to the developer who commented on the feasibility and cost of making the change. If it was feasible, the developer proposed a design that was then reviewed by MME participants with special interests in the system, e.g., security, data collection, user interface, or performance. Finally, the proposed change was presented to a Configuration Control Board. If approved, the implementation of the change would take place. This procedure was intended to provide control over the changes that were made in the system, so that it would be stable and not subject to unnecessary or disruptive changes without sound basis.

SECTION 5
CINCPAC/J3 MESSAGE HANDLING

5.1 Introduction

Even though it was specifically tailored to parallel, as much as possible, the paper message environment, the level of automation provided as a result of the Military Message Experiment had a substantial impact on the manner in which CINCPAC J3 dealt with its daily message traffic and message files. In this section, a comparison will be made of the J3 message handling during a baseline period prior to the introduction of the SIGMA system (late 1977) and later during the period of peak experimental activity from February to June 1979.

The overall message volume was rather stable during the periods of concern. Table 8 shows the average volume of traffic both into and out of J3. While there were some variations in volume between 1977 and 1979, the only major fluctuations resulted from crisis and exercise periods. At CINCPAC messages transmitted via the AUTODIN system are received at the Local Digital Message Exchange (LDMX) in the communications center. In the manual system the messages are sorted, copied, and placed in pigeonholes for pickup by representatives of the directorates. In the directorate administrative office (J301), each ACTION message is assigned to a division or branch. Both ACTION messages and information (INFO) messages are then sorted and either delivered to the division or put into pigeonholes for subsequent pickup by division clerical personnel. With SIGMA, message citations (summaries) were delivered directly to the J301 "pending file" via an electrical connection to the LDMX. Concurrently, each message was delivered to a datefile, a file of messages with a common date of origin. Messages in this file could be accessed directly by any of the system users. When J301 routed a message, its citation was delivered to the recipient's pending file. The user could see the message itself by issuing a "display message" instruction.

TABLE 8. Typical Message Handling Statistics

	Normal Operations	Crisis/Exercise
Incoming		
CINCPAC Total	4,000 per week	11,000 per week
J3 Total	2,000	8,000
ACTION/COG	800	3,600
Outgoing		
J3 Total	120 per week	235 per week
Readdressals	55	105
Originating	65	130

Comparisons of the number of messages filed, referenced and retrieved using the manual and computer-aided systems are difficult because the paper system continued to be used throughout the experiment. Both systems were used by nearly everyone; each system served a useful purpose. Messages being saved for future use were kept in files. These files, depending on the system, also contained other types of information such as notes, letters, memos, etc. In the manual system the files contained paper copies of messages of interest. In SIGMA, each message file contained a collection of pointers to the messages in the form of summaries. The complete messages were kept in a central data base. Although the users actually manipulated these summaries or entries, they tended to think that they were manipulating the messages themselves. SIGMA files also contained informal notes and formal memos that had been created using the system.

Messages may be drafted in response to other messages, in response to nonmessage communications, or to initiate an action or project. They must be coordinated with other members of J3 and CINCPAC, so that those who may be affected by the message, or those who are knowledgeable about the topic it covers, have a chance to approve or revise the message content. Other types of communications, such as letters or memos, are also used.

At the time SIGMA was installed at CINCPAC, the only automated text handling aids in use in J3 were magnetic tape typewriters. Not all of the offices were equipped with these typewriters. For many of the staff, changes in the text of a message resulted in having the message typed and retyped manually. SIGMA was designed for the reception, manipulation, and creation of messages; it was not designed as a word processing system. However, it provided basic text editing features needed to create and edit relatively short messages in standard military formats. Text could also be created and saved independently as "text objects;" these could be incorporated into messages later. In addition, text could be extracted from messages and saved as text objects for future use. These basic word processing capabilities found their way into widespread use by the J3 staff.

Figures 9 and 10 provide a graphical representation of CINCPAC/J3 message flow using the manual and the SIGMA systems. Note that the manual flow depicted in Figure 9 continued to shadow the automated flow throughout the experiment. The following subsections provide some insight into both the quantitative and qualitative differences between the manual and automated system. They concentrate on the basic activities of message distribution, message retrieval and use, file use and maintenance, and outgoing message processing.

5.2 Message Distribution

Under the manual system, batches of messages were picked up seven times daily at the communications center and brought back to the J301 office. Each trip to the communications center took about 15 minutes of a clerk's time. Responsibility was then assigned to a division or branch for each incoming ACTION message by J301. ACTION and information (INFO) messages were sorted and either delivered to the division or picked up by division clerical personnel. The J301 copies of all the messages were filed according to the

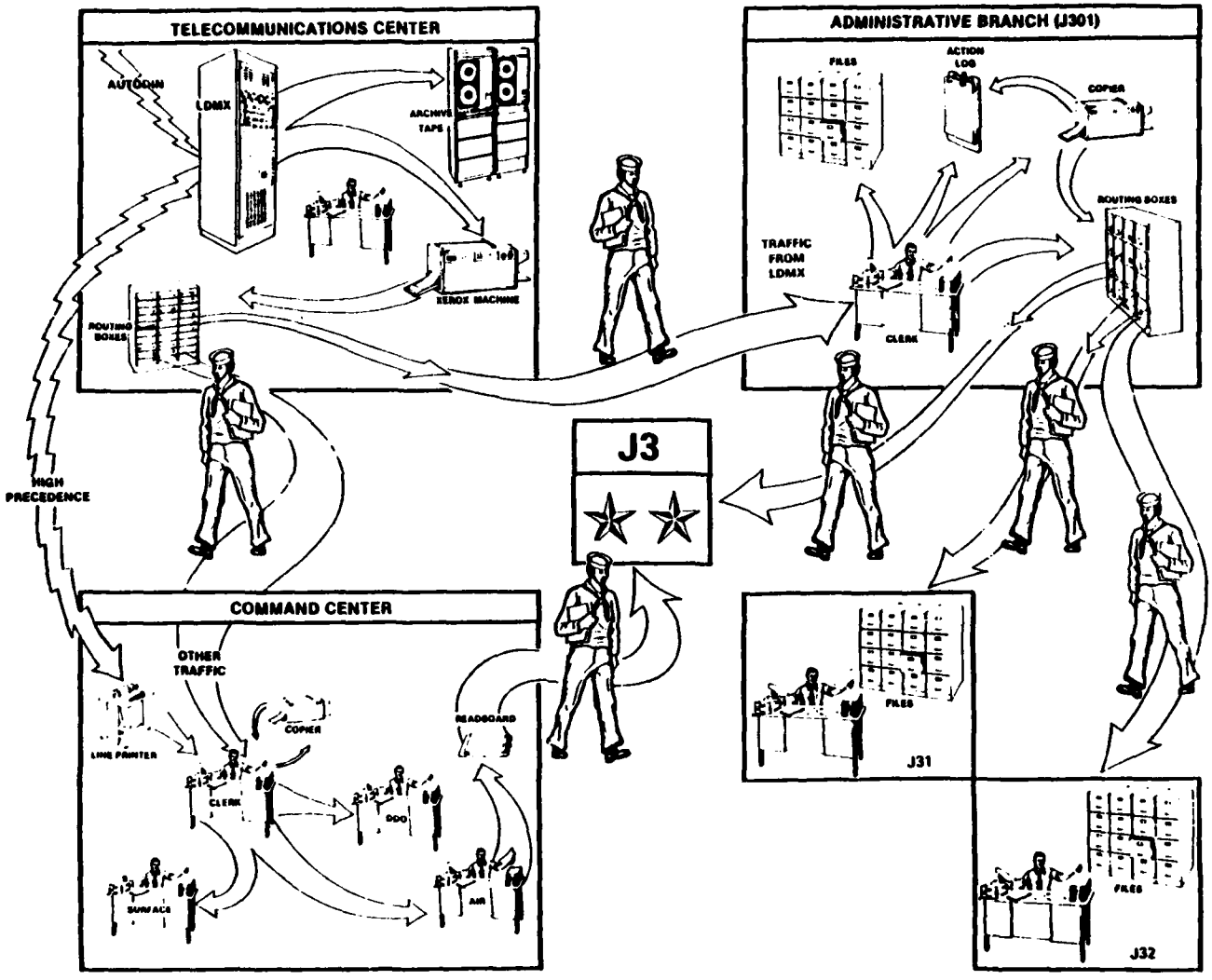


FIGURE 9. Manual Message Distribution

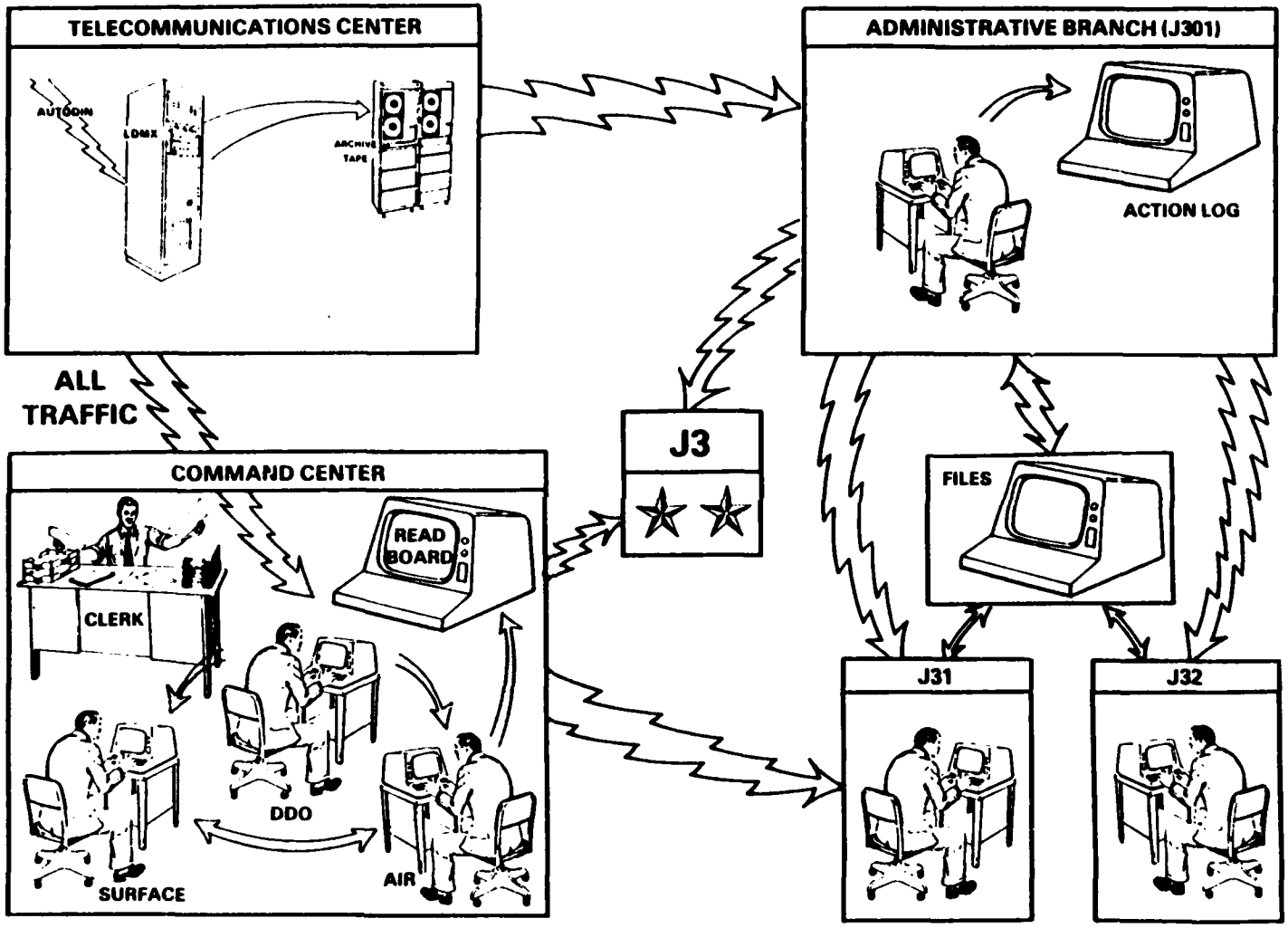


FIGURE 10. Automated Message Distribution

originator's date-time group (DTG). During the baseline data collection period, a daily average of 121 messages were distributed during the day time shift. J301's processing of a batch of messages took an average of 89.5 minutes a day, or an average of 0.74 minutes per message. This does not include the time spent going to the communications center to pick up the message batches or the time spent delivering the processed messages to the appropriate divisions.

Using SIGMA, J301 usually began the day by displaying the pending file and moving J3 INFO messages to a file called the "Today" file. Foreign Broadcast Information Service (FBIS) messages were deleted. When the pending file had been cleared of these messages, the distribution task began. To distribute messages, the J301 user executed a sequence of three instructions. The first selected a set of messages of interest to a particular division (based on criteria contained in the "selector" it had specified). The second routed the messages for ACTION to that division, forwarded copies for information to other divisions, filed a J301 copy, if desired, and deleted the set of messages from J301's pending file. The third instruction displayed to the user the remaining set of messages that had not yet been processed. This sequence of instructions was repeated until all predefined selectors had been used. The remaining message summaries were scanned, with J301 often making routing decisions on the basis of the summary itself. About 13% of all the messages were actually read by J301, presumably to help in routing decisions. During the period from 22 February though 9 June 1979, J301 distributed an average of 274 messages daily using SIGMA. Distribution tasks averaged 76 minutes per day, an average of 0.28 minutes per message. See Table 11. These figures include messages delivered to the pending file throughout the day and evening shifts. In order to make the comparisons meaningful, the messages received on the evening shift are included in the count for the manual system as was done for the SIGMA count. Thus, the count in Table 11 for messages received by the manual system is substantially higher than the average of 121 per day shift.

TABLE 11. J301 Routing Effort

	Manual	Sigma	Difference (%)
Mean # msgs per day	357	274	-23
Mean time per day	207 min	76	-63
Mean time per msg	0.58 min (35 sec)	0.28 min (17 sec)	-51

Using the manual system, the time it takes a message to get from the LDMX to the division or branch office is affected by the communications center processing time, J301 processing time, and the wait at each point for the message to be picked up or delivered. During the baseline period, the average message age at time of delivery was estimated to be 124 minutes for a Priority message, and 193 minutes for a routine message. The greatest amount of time (89 minutes and 158 minutes respectively) was spent between LDMX arrival and pickup by J301. Using SIGMA, the message delivery time was affected by LDMX-to-SIGMA transmission time, and the wait at J301 for the message to be processed. In either system, there is likely to be a delay in the recipient's office, between the time of message arrival and the time the recipient actually sees the message.

Data were collected on the time it took about 30 messages to reach J301 after their arrival at the LDMX. Because the LDMX processes messages by precedence, priority messages reached SIGMA about 4 minutes faster than routine messages. J301 checked its SIGMA pending file periodically and the messages received were distributed at random intervals. The average time between distribution periods during the FEU was 46.6 minutes.

Data were also collected on the amount of time it took for a message to be routed from one user to another. Delivery time was related to the number of messages sent. For small batches (1-4 messages), the messages were delivered in 1.3 to 2.3 minutes. For larger batches, messages were delivered in 3.3 to 5.8 minutes. A comparison of the manual and SIGMA message distribution times can be made using Table 12.

TABLE 12. Estimated Message Age in Minutes When Delivered to Division/Branch

	Baseline		SIGMA Use	
Message Precedence:	Priority	Routine	Priority	Routine
TCC processing	57.5	76.3	6.2	10.1
Wait for pickup	31.5	81.7	—	—
Age at J301 delivery	89.0	158.0	6.2	10.1
Wait for J301 processing	—	—	23.3	23.3
J301 processing time	25.0	25.0	6.0	6.0
J301-recipient delivery time	10.0	10.0	1.8	1.8
Age when delivered to division/branch	124.0	198.0	37.3	41.2
Difference			-70%	-79%

Using SIGMA, J301's effort in distributing messages was cut in half and the message were delivered to the ultimate user over 70% faster. The use of selectors to find groups of messages for a single division and the use of the single "route" instruction to accomplish distribution, filing, and deletion were important factors in this reduction. It should be noted that changes in telecommunications policies or in system design could have significant effects on J301-like activities. Consistent use of office codes, subject lines, and reference lines by all services would permit a system design based on automatic distribution to the division, branch, or office level. This would reduce the effort in distributing messages and would speed delivery.

5.3 Message Retrieval and Use

Under the manual system, message recipients normally flip through a stack of newly arrived messages, pulling out or stopping to read those of particular interest. This process could be accomplished very quickly, with decisions to keep messages for future use sometimes based on format of the text rather than the content of the message. About 30% of the users responding to a CINCPAC-developed survey stated that they felt that using the paper copies of messages for a fast initial review of their recent messages would always be the preferred method.

With SIGMA, users displayed their pending file which contained a list of message summaries including the message subject, DTG, originator, ACTION/INFO status, etc. To see the entire message the user executed a message display instruction and then scrolled through the message. Seventy percent of the users preferred using a computer-aided system for initial message review, even though this was a more time-consuming process than flipping through a stack of paper.

A common style of system use among action officers involved a combination of paper and automated message handling. After initial message review, either on-line or with paper copies, the officers would review the SIGMA summaries and save those messages of interest. Thus they built a data base of messages which were readily available for future retrieval.

During baseline data collection, clerks reported retrieving about two messages a day from project files in response to officers' requests. Sometimes, they had to relay the requests to J301. With SIGMA in use, requests to J301 for messages decreased to less than once a day. While the requirement apparently increased, since clerks reported retrieving an average of four messages a day, they usually retrieved and printed the message directly from SIGMA and gave that printout to the person making the request.

Action officers indicated several advantages of automated versus manual message retrieval. The system offered the ability to search a file for a message or set of messages that met criteria specified by the user without reliance on the exact DTG of a message or a query to a clerk, J301, or the communications center. Messages could be found on the basis of subject, originator, user-specified keyword, ACTION/INFO status, or some combination of these criteria. As new situations developed, it was possible to put together easily sets of messages that had not been related previously. This is

contrasted to the fact that under the manual system, if J301 was not given the exact message DTG, retrieval from paper files was difficult, if not impossible.

A disadvantage of the particular selective retrieval design in SIGMA was that only one file could be searched at a time. The user had to enter separate commands to search multiple files. Many officers commented that they would have liked to be able to specify a multiple file search with a single command. They would have been willing to wait for the system to respond to save the effort of making multiple entries.

The Command Center Watch Team (CCWT) monitored all incoming ACTION messages for J3, so that they could alert the appropriate staff member when a high precedence message arrived, or build a file on a developing situation. The air desk officer was also responsible for building the readboard for the J3. It contained messages thought to be of special interest to the J3 and messages of certain categories, such as those originated within J3. With the manual system a clerk monitored the DCT2000 printer and a pneumatic tube terminus in the Command Center and delivered the messages to the appropriate action officer. This procedure was continued when SIGMA was in use. With SIGMA, duty officers set up alert critera so they would be notified when high precedence messages arrived. They left their terminals logged on throughout the shift so they would receive the alerts as they were delivered. It was important to the duty officers to check all incoming messages. Therefore, during their initial message review they usually did not use selectors for finding a particular set of messages. Instead, they scanned each message summary individually. At the air desk, each message summary was deleted individually from the file. At the surface desk, message summaries were often viewed and deleted in groups. For retrievals the CCWT had many of the habits and preferences of the action officers. They used selective retrieval to find messages in their files, and used the datefiles to find for themselves older messages of interest. Because of their direct links, however, these officers were more likely than the action officers to request message retrieval from the communications center.

At a somewhat higher level in the organization, the division chiefs liked having access to the readboards created each day for the director. In the paper system, the readboards, which contained messages of special interest to the J3, were not generally available to division chiefs due to the time necessary to reproduce the readboards prior to the morning briefing. SIGMA, however, provided the capability to distribute the readboards prior to the briefing. The chiefs felt it was an advantage for them to see which messages had been brought to the attention of the director. They felt they could be better prepared to discuss events with the J3 when they had seen the readboard contents themselves.

Computer-aided message retrieval provided numerous advantages to the system users. These advantages were difficult to quantify, particularly because the paper system was maintained in parallel. However, the observed patterns of system use coupled with responses on questionnaires and interviews lead to these conclusions. The availability of the on-line datefiles was an important feature. They enabled users to retrieve older messages without relying on the availability of a clerk or the communications center. They

also made it possible for users to find messages not previously thought to be of interest, and to build new files as situations arose. Users could also retrieve messages of interest on their own initiative, without depending on someone else to distribute the messages to them. Selective retrieval based on one or more message characteristics enabled users to find messages of interest without having to know the DTG or having to scan the entire message file.

5.4 File Use and Maintenance

J301 maintained a file of paper copies of each message received for 30 days in DTG order. Basic maintenance of this file took about 40 minutes per day during the baseline data collection period. With SIGMA, all incoming messages were automatically filed in the appropriate datefile. J301 typically owned (i.e., was responsible for the maintenance of) around 15 SIGMA files. The general flow of messages through J301 required three files for each day's operations. Messages were received in a J301 pending file, and copies retained in an action log file for ACTION messages or the "today file" for INFO messages. Maintaining these files was not a time consuming task. In other branches and divisions, the amount of filing varied considerably from day to day during the baseline data collection period. The clerical personnel actively maintained around 10 files each, although they had access to many more. When filing was done it usually took less than 20 minutes a day. To accommodate a need for keeping some messages in several files, approximately 10% of the messages had to be copied. With SIGMA in use, the amount of file maintenance required of the clerks decreased somewhat, especially at the branch level where officers maintained many of their own files. Administrative support personnel used the system to retrieve messages requested by a division or branch chief, and to print it for their use. These retrievals were often made from the SIGMA datefiles.

With the manual system, action officers kept current material themselves, often in folders on their desks, and relied on the clerks to maintain older files of information. Most of the action officers were directly responsible for 20 or fewer files, and spent less than 2 hours a week on file maintenance activities. Of all the messages they received, most officers reported keeping between 15 and 50 messages a week. With SIGMA, the officers tended to do more of their own filing, since they created files and saved messages in the course of reviewing the incoming messages. Many of the files continued to be shared among persons in a branch working a problem. Depending on the incoming message load, action officers averaged between 30 and 60 minutes a day actively using message files. This included time spent scanning incoming messages in the pending file as well as time spent moving messages into other files, deleting messages, etc. A "comment" capability was provided to enable users to write notes to themselves or to others and associate these with a message. This facility received little use. The integration of on-line and off-line materials was usually accomplished by printing a message and filing it in a paper file.

In the Command Center the number of files used was related to the duty desk. During manual operation (the baseline data collection period), the surface desk reported keeping the largest number of files, over 100, with most of them project-oriented. The air desk reported maintaining around 50 files,

and the DDO kept around 10. These duty officers also made many more duplicate copies of messages, since they passed many along to action officers responsible for a particular area as well as keeping copies for themselves. The number of files each officer maintained using SIGMA varied, but was fairly small. At the end of the evaluation, the air desk officers had 18 files, the DDO had 3 files, and the surface desk 5 files. During late February-early June 1979, the air desk officers as a group used 122 different files; the surface desk used 157 files, and the DDOs used 26 files. These included the datefiles and readboards as well as project files related to each desk. The air desk officers averaged about 3 hours a day of active file use. The surface desk officers averaged 1.5 hours, while the DDOs averaged 0.5 hours of active file use a day. Use by the Joint Reconnaissance Center (JRC) was similar to that of the surface desk officers. They accessed 136 different files during the period of use, and had an average of 1.5 hours a day of active file use. The command center clerks were not involved heavily in file maintenance during the baseline period. They maintained only two files, and most spent less than an hour a week on file maintenance. Their pattern of SIGMA use was similarly light. The duty officers, rather than their clerks, maintained the files. The clerks averaged less than 30 minutes a day of active file use, and accessed 13 files throughout the peak use period.

The use of SIGMA resulted in a slight shift in file maintenance activities. Action officers moved messages from file to file and deleted messages in files more than the clerks and clerical level administrative personnel. These maintenance activities were often accomplished in connection with message review. All users felt it important for them to have control over the files they used, in terms of creating the files, organizing material within them, deleting them, and controlling access to the files. On-line files did have a disadvantage over paper files. Contents of the on-line files were limited to messages, memos, and notes that were received or created on-line. They could not include hand-written notes, diagrams, directories, and the like that might be found in paper files.

5.5 Outgoing Message Activity

The J3 staff did not generate a large number of original outgoing messages during normal periods. Therefore, during the first two weeks of August 1979, SIGMA users were asked to use SIGMA whenever possible for creating, coordinating, and releasing outgoing messages. The bulk of the SIGMA data discussed in this section was collected during this two-week period, and comparisons are drawn against the baseline period. During one two-week period of baseline data collection, twenty-two offices reported creating a total of twenty-two outgoing messages for release and transmission over AUTODIN. Baseline data showed that the majority of the staff spent less than one hour a day on message creation and editing. Clerks in branch offices, who support from three to five officers, reported spending from one-half to two hours a day typing messages. In the manual system, messages are typed onto machine-readable (OCR) forms and then carried to the LDMX for subsequent transmission. Command Center duty officers originated very few outgoing messages. These officers also reported creating less than one message a day. The typing effort reported by their clerks was also low; they reported typing an average of one message a shift, and averaged 5 to 14 minutes per message.

They also did a small amount of letter and memo typing. See section 5.5.3 for a discussion of the problems associated with a message in the manual system after it is released.

5.5.1 Readdressals

In addition to originating messages, the staff also readdressed messages. The purpose of a readdressal is to send a received message to an addressee outside of CINCPAC. Readdressals are very short, formatted memoranda sent to the Telecommunication Center. During the baseline data collection period, users reported this to be a cumbersome process, involving much time and paperwork.

Activity during the intensive two-week period of SIGMA use focused on outgoing messages; 29% of all the outgoing messages that participating J3 staff created were done on SIGMA. The largest proportion of these were readdressals. Although 18% of their original messages were created with SIGMA, nearly twice as many, or 35% of the readdressals were done on SIGMA. Looking at this another way, 79% of the messages created on SIGMA were readdressals. Many users reported that they preferred doing readdressals on SIGMA. Unlike the time-consuming manual process, which involved writing a complete new readdressal, readdressals were handled quickly and easily on SIGMA. The "readdress entry" instruction was provided on a function key. When the user hit this key he received a partially filled out form. The user only had to add the new addresses, designate the coordinators, and the message precedence if different from the system default of ROUTINE.

Many of the users' reservations about creating messages on-line were related not to the editing facilities offered, but to the coordination and release functions that will be discussed shortly. Although over 70% of the outgoing AUTODIN messages were created using manual procedures, 95% of the users reported they preferred using automated procedures for message creation and editing. Their preference was based on the efficiency and speed of the system, particularly as a word processor. The use of preformatted messages, with each field labeled and some automatically filled in, and the ability to copy text from one message to another were cited as useful aids. One user reported that he had greater confidence in the accuracy of his messages which contained data tables taken from other messages because they did not have to be retyped. Other features users rated highly desirable included user control over text formatting, storage of messages in draft form, and reclassification of messages in their entirety or by message field.

5.5.2 Coordination

AUTODIN messages, including readdressals, must be coordinated before release and transmission to ensure that the contents are accurate and represent an agreed-upon position among the members of CINCPAC who may be involved in the message. Messages sent for coordination are usually accompanied by two or three pieces of reference material. These may be other messages, memos or documents. The coordinators may also want to talk to the originator to gain additional information. They may approve the message as is or with changes they propose. Or, they may disapprove the message.

Although 75% of the SIGMA users responding to a questionnaire said they preferred automated to manual procedures for coordinating messages, SIGMA was not often used for message coordination. One difficulty encountered with on-line coordination during the evauation was the inability to put together a complete coordination package when materials not on-line were needed to back up the message. Another problem was the relatively small user population; often coordinators were not system users. Finally, users often lacked confidence that the coordinators would check their files frequently. Message originators felt their message would get faster attention if they were hand carried to the coordinators, and if they as authors were on hand to answer questions. Some of these problems would be resolved in an operational system which was implemented throughout an organization. By having everyone on-line and accustomed to using the system routinely for message tasks, problems of getting a coordinator's attention would be alleviated. However, the problem of integrating on-line and off-line materials must be considered.

The users did like some of the features of on-line coordination. The most highly rated feature was parallel coordination. With manual procedures a single coordination package is put together and circulated one at a time among the coordinators. With SIGMA all coordinators could be sent a notification about the message at once, and they could access it independently of each other. (They could see each other's comments if the commenter authorized access.)

5.5.3 Release

When the coordination procedure is complete the message is shown to someone with authority to approve formally, or release, the message for transmission. Most releasing is done by the director or his deputy. Occasionally division chiefs or the DDO will release messages. Message release is a fairly routine task. By the time the message reaches the releaser it has been through the coordination process; the releaser may review the message for his own information, but generally he does not make changes to the message. Using SIGMA, release by authorized users was accomplished with the stroke of a single function key.

With the manual system, after a message has been released it is taken to the communications center where it is put into an OCR reader. If the message is read successfully, it is transmitted. If not, the OCR operator tries again. With repeated failures the message may be fixed at the communications center, or it may be sent back to the originator for retyping. At times the rejection rate is as high as 80-90% on the first try. Processing of a sample of outgoing messages during baseline data collection took an average of 70 minutes for a priority message and 131 minutes for a routine message. This time began when the message arrived at the communications center, and included the time spent waiting for a clerk's attention, his attempts to have the message accepted by the OCR, and associated LDMX processing time.

Although no data were collected that measured total SIGMA and LDMX processing time for a released message, measurements were made of the message transfer time between SIGMA files; the average is four minutes. After an action officer released an output message on SIGMA, it was transferred to a

separate SIGMA file for transmission to the LDMX. Because these messages were subject only to the average four-minute file transfer delay and not to the manual delivery, holding for messenger, and OCR delays of the manual system, outgoing messages were processed more quickly with the automated system.

SECTION 6
ANALYSIS OF NORMAL OPERATIONS

6.1 Introduction

Section 5 contains a description of the flow of message traffic in the baseline (before SIGMA) and the automated (SIGMA) systems. A complete description of the system before automation is given in the Baseline Data Report [30]. The general message traffic flow and the use of SIGMA after automation are reviewed in the following paragraphs.

6.2 Initial Processing

AUTODIN messages for CINCPAC are received from the AUTODIN Service Center at the Camp Smith LDMX (Local Digital Message Exchange). The LDMX transmits high precedence messages directly to the CINCPAC Command Center in addition to the normal distribution. Messages that the LDMX determined should be routed to the Operations Directorate (J3) for ACTION or Information (INFO) were transmitted electrically to the SIGMA system. (Backup paper copies were generated by the LDMX and picked up later by J3 personnel.)

Once a message was received by SIGMA, it was placed in the SIGMA message file and protected from changes. A summary of the message was placed in the Administrative Branch's (J301) pending file (SIGMA's version of an "electronic in-box") and in the datefile (a file of messages with a common date of origin). SIGMA screened incoming messages for certain keywords in the subject field that indicate that the message should not receive wide distribution. These messages were not placed in the datefile but were delivered directly to designated users through a limited distribution process.

6.3 Administrative Branch (J301)

J301 periodically scanned the pending file and distributed the summaries (or citations) to the appropriate division within J3 for Action or Info. J301's distribution caused the message summary to be placed in a user's pending file. J301 personnel usually arrived before the start of the normal workday to take care of distributing the messages that arrived overnight. One of the staff would log on, display the pending file, move all the INFO messages to another file, delete the Foreign Broadcast Information Service (FBIS) messages, and distribute the remaining messages.

J301 distributed messages to each division based on a mutually developed profile for each division. This profile consisted of a set of predefined criteria (called a selector in SIGMA) that selected messages based on message DTG and/or Originator and/or keywords in subject, etc. Once the messages had been selected, J301 executed a SIGMA command to assign ACTION to the selected division, distribute information copies to other divisions, file copies in a J301 file, if desired, and delete the messages from J301's pending file. J301 then displayed summaries of the remaining messages and repeated these three steps until all the predefined selectors were used. J301 then displayed the remaining message summaries and distributed them individually. J301 viewed

the actual message (in addition to the summary) for only 13% of the actual messages in the pending file. It is probable that this was done in most cases to aid in determining proper distribution.

J301's message distribution function could easily have been changed to operate on a "by-exception" basis. The system could have automatically deleted the FBIS, transferred INFO copies to another file, executed all the pre-stored selectors, distributed the messages, and then alerted J301 to any remaining messages that needed attention.

The ACTION assignments were maintained in a system file that could be checked to determine the status at any time.

6.4 Action Officers

After a message (actually a summary) was delivered to a user's pending file, it was his responsibility to take the proper action. If the user was logged in at the time, the information that a message had arrived was placed at the top of his screen. Most users did not maintain a constant vigil at the terminal, but periodically processed their pending files. The action officers maintained and used SIGMA message files; they spent an average of 6-30 minutes a day using message files.

Once a message was received by an action officer, he could read it, file it in one of his personal SIGMA files, take action on it, forward it to another user, "sell" the ACTION assignment to another user, delete it, comment on it, print it, reply to it, readdress it, or perform some reasonable combination of these actions.

Some action officers used selectors to find groups of messages, and some selected messages by scanning the summary. Most action officers could determine which messages they wanted to display by looking at the summaries. Thus, they deleted some messages from their pending file without ever reading them.

Many action officers did not wait for J301 to route the messages. They accessed the datefile directly and selected those messages that were of possible interest. Thus, they were able to use more flexible selection criteria then the profile being used by J301, and they were able to get the messages earlier. Toward the end of the experiment, it was clear that J301's manual routing function was becoming less important, and that future systems could rely on automated routing systems that could be changed easily by the users.

SIGMA's implementation of the datefile system divided the set of messages stored on the system into a logical file of message summaries for each day. The effect was that a user had to enter a separate query to search each file. Had the experiment continued for a longer period, this would have been changed to allow queries to specify a date-time period unconstrained by day boundaries.

6.5 Command Center

The system in use prior to SIGMA was maintained as a backup for the Command Center Watch Team. High precedence messages were transmitted directly from the LDMX to the printer in the Command Center. Paper copies of all messages for the Command Center were delivered from the communications center via a pneumatic tube. Thus, the changes in message distribution after SIGMA were not as dramatic to the Command Center Watch Team as for the action officers. The CCWT did use SIGMA to build and access files and to build the readboard for J3. Except for their reliance on the printer for delivery of high-precedence traffic, the use of the system by the CCWT was about the same as that of action officers.

The air desk officer within the CCWT has the responsibility for building the readboard for the Director. During the experiment he used SIGMA to do this; therefore, those functions used in support of file maintenance were the most valuable ones to the air desk officers. Every shift, the officer logged on and carefully went through the air pending file. (The air desk received copies of all the incoming messages for J3.) He deleted the messages of no interest and filed or made copies of those which had to be included in the daily readboards.

6.6 General Use

CINCPAC J3 is typical in that the directorate receives more messages than it transmits. But the number of man-hours per message to create, coordinate, and release an outgoing message is higher than the number of man-hours per message to process incoming messages. Difficulties were encountered in designing and implementing a satisfactory system for coordinating outgoing messages. The SIGMA designers and the CINCPAC users analyzed the manual coordination process and, by the end of the experiment, had devised a system that was beginning to be used by the users. The major problems were:

(a) usually, not all persons needed for coordination of an outgoing message were system users;

(b) all coordinators might not be logged on;

(c) some material needed for background for coordinators was not on the automated system; and

(d) some users believed the social intercourse of face-to-face coordination was needed.

SIGMA provided a capability to create informal notes and formal memos for intra-directorate communications. Notes and memos were used extensively by the users toward the end of the experiment. The principal users were action officers and members of the CCWT. SIGMA was also used as an office word processing system to generate text objects that were used in briefings, draft letters, notes on projects, status of action, and day-logs to aid in watch shift transitions.

6.7 Use of Various System Functions

To aid in determining the functions needed in future message handling systems, this section analyzes the use of various SIGMA functions by the users. Keep in mind that when users route or delete messages or manipulate file entries, they are actually working with message summaries that are the users' access media to the messages. Users cannot modify or delete incoming messages or outgoing messages after they are released. Table 13 is reproduced from [9]; it lists the SIGMA instructions and function keys.

In Table 14, the instructions executed by all users are shown. For each type of instruction, the percentage of the total number of instructions executed is shown.

The "delete message" instruction was the most widely used instruction (25% of the total). It was important for file maintenance and useful to all types of users. It was especially useful to Command Center users. They received copies of all the incoming messages for J3 but were interested in only a small percentage of these. The instruction could be entered by pushing a function key or by typing it in. If entered by function key, only one message could be deleted at a time; if typed in, one or more messages could be deleted with the one execution. Both implementations of "delete message" were used widely and should be included in future systems.

"Display file" was the second most widely used instruction (16% of the total). It was executed by every user. When a user first logged on, he had to type "display file pending" in order to see the summary of his incoming messages. In addition, "display file" instructions were used to support the users' message retrievals. Retrievals were made on the file that had been "opened" by a "display file" instruction. The concept of different files and the ability to display summaries of messages within a file are key features that must be included in future systems.

"Display message" and "view message" instructions made up 9% and 6% respectively of the total instructions executed. These instructions enabled the user to read and edit his messages, capabilities fundamental to any automated message-handling system. Both the display window and the view window were used for reading on-line objects. (The display window was a read-and-edit window; the view window was a read-only window.) Users generally had a preference for one of the two windows. Command Center users and J301 used the view window almost exclusively; they liked to have the file and a message from the file displayed simultaneously. Action officers, clerks and administrative personnel preferred using the display window.

TABLE 13. SIGMA Typed Instructions and Function Keys

Instructions

ABORT	DISPLAY NEXT	PICKUP
ACTION	EMPTY FILE	PRINT
AUGMENT	EXERCISE	PUT
BACKUP ALL	FILE	READDRESS
COMMENT	FIND BOTTOM	RECLASSIFY
COPY TEXT	FIND ENTRY	REPLY
CREATE	FIND STRING	RESET ALERTS
CREATE FILE	FIND TOP	RESTORE
CREATE MESSAGE	FORWARD	RESTRICT
CREATE SELECTOR	GET	ROUTE
CREATE TEXT	HIGHLIGHT	SORT
DELETE	IDENTIFY	SYSTEM NEWS
DELETE ENTRY	KEYWORD	VIEW
DELETE FILE	LESSON	VIEW KEYWORDS
DIRECTORY	LOG OFF	VIEW VERSION
DISPLAY	MOVE	
DISPLAY FILE	MOVE TEXT	

Function Keys

ALERT ON/OFF	ESC	REPLY NEXT
BACK	EXECUTE	RESET
BACKUP ONE	EXPAND	RETURN
CANCEL	FINISH	ROLL DOWN
CHOP	FWD	ROLL UP
CHOP NO	GO TO NEXT	SAVE
CHOP YES	HELP	SHOW FILE
CLEAR VIEW	HERE	SHOW MESSAGE
CNTL	MOVE	SHOW TEXT
COORDINATE	NO	UP WINDOW
COPY	ONLINE	UPDATE
CURRENT ENTRY	PICKUP	VIEW DISPLAY
DEL	PROMPT	WORD LEFT
DISPLAY ENTRY	PUT	WORD RIGHT
DISPLAY NEXT	RELEASE	YES
DOWN WINDOW	REPLY ENTRY	

TABLE 14. Percent of Total Instructions (All Users)
22 February - 29 September 1979

delete message	25%	find entry	0.4%
display file	16%	empty/sort file	0.4%
display message	9%	coordinate message	0.3%
view message	6%	forward message	0.3%
clear view window	5%	comment message	0.3%
finish	5%	create message	0.2%
file/move	6%	readdressal	0.2%
restrict/augment	4%	chop message	0.1%
route message	4%	create file	0.1%
print	4%	view selector	0.1%
alert on/off or reset alerts	2%	reply message	*
backup	2%	action message	*
display text	1%	highlight message	*
view directory	1%	create selector	*
save/update	1%	keyword	*
copy/move/pickup/put text	1%	copy message	*
create message	0.4%	file/move and sort	*
release message	0.4%	go to	*
find string	0.4%	others	2%

* indicates less than 0.05%

Note: Although some of the instructions received very little general use, they are necessary for any future automated message handling systems; the importance and use of each of the instructions are discussed in the text.

A future AMHS should have multiple windows. In creating messages, it is useful to look at other messages and text objects at the same time the new message is displayed. Text can then be picked up and transferred to the new message with less chance of error. In replying to a message, it is convenient to have access to that message and others as references. In fact, many users did not use SIGMA for message creation because they could not have several relevant messages immediately at hand. Multiple windows are also useful for coordinating outgoing messages.

The "clear view window" and "finish" instructions were used moderately (5% each). These instructions were used by the user to complete work. "Clear view window" removed an object from the view window and expanded the display window to include the space that was being used for viewing. "Finish" removed an object from the display window and made permanent the changes that had been made to the object. Prior to doing a "finish" the changes could be discarded.

The "file" and "move" instructions were used moderately (6% of the total). The "file" instruction put a copy of a message into another file. The "move" instruction was a combination of "file" and "delete;" it copied a message into another file and deleted it from the current file. The "move" instruction was preferred seven to one for transferring messages from file to file. In general, the instructions which combined two or more functions in a single instruction such as "move" or "route" (see below) were well-received and widely used by SIGMA users.

"Restrict" and "augment" are used in selecting a subset of messages from a file. They received moderate use (4% of total). The subset of messages selected by these commands is determined by a group of "Selectors" connected by logical ANDs. A selector specifies a field and the values that can be used as selectors. The following is an example of items that can be included in a selector.

FROM FLEWEACEN, ACTION J31, BEFORE 021745Z OCT 79, PRECEDENCE Z, SECURITY SECRET, SUBJECT ATTACK.

This would select those messages that are from FLEWEACEN (the Fleet Weather Center) and have been assigned to J31 for ACTION and have a DTG prior to 021745Z Oct 79 and with a precedence of Z and with a security classification of SECRET and with the word attack in the subject line. "Restrict" restricts the currently selected entries to only those meeting the selection criteria; "augment" adds to the currently selected entries those that meet the selection criteria. Some form of flexible message selection equivalent to restrict and augment is necessary for a future AMHS.

"Route" is an instruction used primarily by one user group. It performs four operations on a group of messages. It assigns action on them, forwards them for information, files them in designated files, and deletes them from the pending file if designated to do so. "Route" made up 4% of all the instructions executed by all users, but about 83% of those were executed by J301. Most of the remaining 17% were executed by the Executive Officer (XO) during the two exercises.

A message distribution function is essential to a future AMHS. If routing is not done automatically, then the equivalent to a "route" instruction is a necessity.

It was often necessary for users to get hardcopies of messages by using the "print" instruction. This instruction was used by clerks and administrative personnel whose superiors did not have a terminal available and by all users after locating an old message. It was essential for users who preferred working with paper copies of messages. Text objects were also printed, especially by the presentations branch whose briefings were prepared as SIGMA text objects. "Print" instructions made up about 4% of the total instructions; over 12,000 objects were printed throughout the experiment.

The alert capability was very important to the users. There is no way to correlate the use of the "alert on/off" or the "reset alerts" to the importance of the receipt of an alert. The "alert on" instruction displays in the view window the list of received messages that meet the user's criteria for alert; "alert off" restores the previous content of the view window. "Reset alerts" clears the alert list. Most of the CINCPAC users believe an alert capability is a necessity in an AMHS.

There were several functions which were used infrequently but were critical to a particular task. "Coordinate message," "chop message," and "release message" are examples of commands that are essential to message preparation and release. Some functions were implemented late in the experiment and, thus, may have had little use (e.g., the "find top" command that saves a user the trouble of scrolling back through a long file to the first message).

Several functions were executed infrequently because they were implemented in an inconvenient manner (e.g., highlight and keyword).

SECTION 7
ANALYSIS OF EXERCISE OPERATIONS

7.1 Introduction

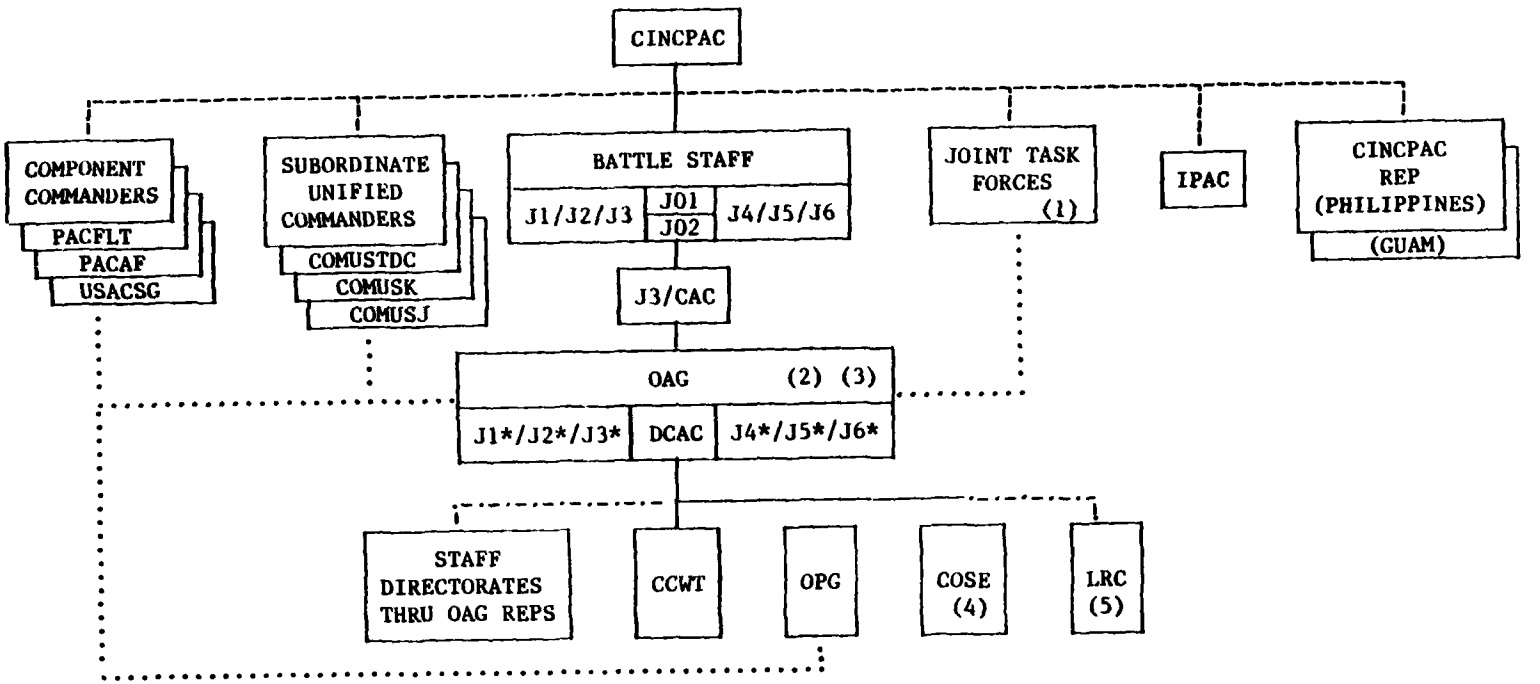
During an exercise or crisis, the CINCPAC staff reacts in accordance with their standard procedures (CINCPACINST 3120.2B, 1 March 1977 applied during the MME period). When a situation requiring crisis action (or an appropriate state in an exercise) is recognized by the Command Center Watch Team (CCWT), several events occur. First the Crisis Action Coordinator (CAC), typically J3, or his deputy, convenes the Operations Action Group (OAG) in the Command Center. An Operations Planning Group (OPG) is also established, and an area is set aside for the Current Operations Support Element (COSE). The OAG acts as the focal point for the crisis/exercise activity; the other groups support the OAG as necessary. The CINCPAC organization for crisis action is shown in Figure 15.

7.2 Manual Message Handling in Crisis/Exercise

When crisis/exercise groups are convened, message handling procedures are altered. Crisis or exercise message traffic is usually assigned a keyword designator for message traffic (for example, Exercise Power Play). It is included in the subject line of every crisis or exercise-related message, and added to the list of flagwords in the LDMX. Thereafter, when the LDMX encounters one of these messages, the message is flagged for delivery to the Command Center via the DCT-2000 printer regardless of precedence. The single-part paper in the DCT-2000 printer in the Command Center is changed to five-part paper. The five copies of each message are distributed according to a special exercise distribution list. In addition, twelve copies of each message are sent up through the pneumatic tube from the communications center. The printer copies are available within minutes of the arrival of the message in the LDMX; the copies received through the pneumatic tube usually take twenty to ninety minutes to arrive. For most messages, ACTION responsibility is apparent from the contents of the message, and the appropriate group will proceed to act. Where necessary, ACTION responsibility may be assigned by the J3 representative on the OAG. Most ACTIONs are handled by the Current Operations Support Element, but many are handled by the Operations Planning Group and by the directorate representative on the OAG.

While the crisis or exercise traffic is being handled by the OAG and its support elements, the DDO and the rest of the CCWT remain aware of the crisis actions, but are also responsible for monitoring the non-crisis traffic, using normal procedures.

As during normal operations, some action items require the preparation and transmission of messages. Usually, such messages will be prepared by the support element having the action and will be submitted to the OAG for coordination and release. While taking action on an item, officers often need to read messages referenced in the ACTION message or to read all messages on a given subject. Copies of exercise and crisis traffic are saved (and preserved after the operation is over), but there seldom is time to file these copies



NOTES:

(1) Established when mission to be performed so requires/as directed
(2) Activated in crisis situations on direction of the Chief of Staff
(3) Crisis Action Coordinator (CAC): J3
Deputy CAC: J33 (Primary)
J31 (Alternate)
(4) Staffed as directed by J31
(5) LRC will be activated & staffed as directed by the J4

LEGEND:

---------- Operational Command
_____ Staff Supervision
-.-.-.-.- Staff Support
..... Information/Liaison
* J-Staff Representatives

FIGURE 15. CINCPAC Organization for Crisis Action

except in rough DTG order. As a result, only retrievals by sender and DTG are possible, and even these are not always easy. The Operations Planning Group should coordinate all outgoing crisis/exercise messages. However, because of the press of the situation, some messages are not fully coordinated among all members of the Operations Planning Group.

Significant action items, whether messages or not, are entered into a Status of Actions log maintained on the WWMCCS computer. The following extract from the relevant CINCPAC Instruction describes how this is done:

> Status of Actions (SOA) - A status of actions file will be maintained indicating the staff elements or subordinate commands which are participating in, or supporting, an action. It is the responsibility of each OAG representative/Current Operations Support Element officer to highlight pertinent message traffic for entry into the SOA computer file via the CCWT administrative clerk. Each member of the OAG is also responsible for follow-up, insuring that actions are completed within the established time and for keeping his directorate informed of the status of actions (particularly of final actions) and for coordinating with OAG representatives to ensure pertinent messages have been entered into the SOA file. He will monitor information-entry procedures, updating of the file, and provide assistance to the OAG representative as required. Printouts of the SOA will be available every four hours.

A WWMCCS terminal in the Command Center is used by the administrative clerk supporting the OAG to maintain the Status of Actions Log. A WWMCCS printer in the Command Center is used to print out the log periodically. Copies of this printout are distributed so that each officer can keep track of his action responsibilities. Sometimes, support groups for a crisis operation are convened in other buildings and have the responsibility for supporting their representatives on the OAG and Operations Planning Group. Periodically, couriers take the relevant messages to these groups and return with draft outgoing messages.

7.3 Automated Message Handling During Exercises

The SIGMA system was used heavily during two exercises. In March 1979, it was used as a backup message handling system during exercise Power Play (PP-79). In September 1979, a Simulated Command Post Exercise (SCPX), based on PP-79, was held using SIGMA. These are described in the following paragraphs.

7.3.1 Exercise Power Play 1979 (PP-79)

This exercise was a 24-hour per day Command Post Exercise (CPX) conducted from 6 to 23 March 1979. A Command Post Exercise involves the Commander, his staff, and communications within and among headquarters. CINCPAC participation in the exercise was minimal; there was a skeleton Operations Action Group, but there was no Operations Planning Group and no Logistics Readiness Center.

Fifty SIGMA accounts were established. These included the Crisis Action Coordinator, Deputy Crisis Action Coordinator, Chief of the Operations Action Group, Executive Officer, Assistant Executive Officer, J1 (personnel), J2 (Intelligence), J3 (Operations), J4 (Logistics), J5 (plans), J6 (Communications and Data Processing), J74 (Public Affairs), Exercise Controller, Operations Action Group, Logistics Readiness Center, and Current Operations Support Element. The exercise accounts were opened as one group (i.e., each account was able to access all files, text objects, and selectors in the other accounts). All accounts were opened with release authority for informal notes. The Deputy Crisis Action Coordinator and the Chief of the Operations Action Group had release authority for formal memoranda and AUTODIN messages.

Personnel from the CINCPAC directorates J1, J2, J3, J4, J5, J6, and J74, and from IPAC (Intelligence Center Pacific) who were potential Operations Action Group members were identified together with their message-handling tasks. These personnel were trained to use the SIGMA system with emphasis on the tasks they were expected to perform during the exercise. The training began 1 February 1979 and continued throughout the month of February. It consisted of a one-hour introductory lecture to groups of users, with three hours a day available for hands-on training and experience. Both officers and administrative personnel were trained.

Prior to and during the first week of the exercise, the procedures for the use of SIGMA during the exercise were determined and implemented. The effort included determining and establishing files, text objects, and selectors required by the MME Executive Officer for effective use of the system during the exercise. The remaining members of the exercise team were free to establish their own objects on an individual basis.

SIGMA was used as a secondary message-processing system on a non-interference basis. The MME participation commenced at the beginning of the exercise and continued through the exercise. The MME Executive Officer duplicated the functions of the regular Executive Officer, who utilized the paper message-handling system. SIGMA was used for message distribution, retrieval, coordination, and release. The initial plan called for directorate Action Officers, as time permitted, to duplicate on the MME their paper-system actions. When it was established that SIGMA was in a stable operating condition, they were encouraged to and did use it as their primary system for certain outgoing messages, e.g., those with a 24-hour or longer suspense time.

To support their exercise functions, the MME Executive Officers created and maintained 15 files, 36 text objects, and 2 selectors. The 15 files included a master file for all messages received by the Operations Action Group, a Status of Action Log, a Significant Events Log, and various files for situation reports, JCS Action messages, OAG action requests to the JCS or other Headquarters, CINCPAC directives to subordinate headquarters, MME transmitted messages, paper-system transmitted messages, readdressals, backcopies, etc. The 36 text objects were used mostly to ROUTE incoming messages to different combinations of the exercise accounts for Action and/or Info, FILE in the Master file, and DELETE from the Executive Officer Pending file. The two selectors were the ALERT-SELECTOR that selected and alerted the MME Executive Officer on all incoming messages that were FLASHOVERRIDE, or

FLASH, or IMMEDIATE, or FOR RELEASE, or FOR CHOP, or ACTION, and a selector used to screen files for NOTEs.

All incoming messages on the MME came to the OAG Pending File. The MME Executive Officer reviewed each incoming message summary (or message, if necessary). If there was an OAG action required, he assigned action on the message to the appropriate OAG Action Officer (AO) thus updating the Status of Actions Log. If the message was ACTION on a COG item, he forwarded it to the appropriate OAG Action Officer. All incoming messages were filed in the OAG master file. Important messages were forwarded to the Deputy Crisis Action Coordinator (DCAC). The MME Executive Officer maintained and updated the Significant Events Log as required. He reviewed all outgoing messages, ensured all chops had been made, resolved any non-concurrences, and forwarded the messages to the DCAC for release. If the outgoing message satisfied a pending OAG ACTION or requested ACTION from a co-lateral or higher headquarters, the MME Executive Officer posted the appropriate files. All outgoing OAG messages were filed from the OAG pending file to one of the three outgoing files. The MME Executive Officer ensured that all actions generated from non-message sources were entered into the Status of Actions Log and Significant Events Log as appropriate. He readdressed messages as directed by the Deputy Crisis Action Coordinator. A terminal was available for the Deputy Crisis Action Coordinator, but was rarely used. Releasing outgoing messages, especially readdressals, was the Deputy Crisis Action Coordinator's primary use of the system. The Action Officers had two terminals available for their exclusive use, in addition to the Deputy Crisis Action Coordinator's terminal which was available most of the time. Many Action Officers made extensive use of the MME system during the time available to them when they were not processing actions using the manual system. The J2 and J4 Action Officers created extensive files to support the wide variety of messages received during the exercise.

Normal administrative use of the system continued throughout the exercise. In order to make the system more responsive to the exercise users, the system's scheduling algorithm was changed to give the exercise users higher priority than the other users. Even so, there was a noticeable degradation in system response to exercise users during the period 0600-0900 on normal work days. (This was the period of heaviest use by the normal MME users; they logged on and processed the messages that had arrived in their pending files overnight.)

A CINCPAC SITREP was required, on a 24-hour basis, throughout the exercise. The one-time development of the SITREP on the system demonstrated the utility of interactive capabilities within the system. The different directorates prepared their portions according to a fixed form and forwarded them to the MME Executive Officer who assembled them, prepared the message, and forwarded the message to the Deputy Crisis Action Coordinator for release.

The personnel actually assigned to the exercise team were not those previously identified and trained. Thus, the personnel reporting at the commencement of the exercise had to be trained by the MME Executive Officers and the MME Observer. Those personnel reporting later were trained mostly by the initial members of the exercise team with assistance from the MME Executive

Officers and Observer. In spite of the lack of previous exposure to the MME system, they quickly learned to use the MME in carrying out many of their specific duties. For this exercise, the Operations Action Group was activated with the Deputy Crisis Action Coordinator, Executive Officer, MME Executive Officer, and Action Officers from the J2, J3, J4, J5, and J6 directorates.

Even though there was an excessive amount of system downtime, the MME system, when available, was able to process and distribute messages in a timely manner. The readdressal feature was enthusiastically received by the OAG Action Officers and, once demonstrated, was used for almost all message readdressals. During periods of low OAG activity, some outgoing messages were created and released using SIGMA. On one occasion, the CINCPAC SITREP was prepared on various Action Officer terminals, assembled by the MME Executive Officer on his terminal and released by the Deputy Crisis Action Coordinator on his terminal. The ability to retrieve messages from files was the system feature for which the users expressed the highest degree of preference.

The major problem with the use of the MME system was the unacceptable amount of unscheduled system downtime. The lack of system reliability mandated a backup message-handling system. Initially a very high load average caused by a software failure resulted in lengthy delays in executing commands. Delays also occurred during the coordination or release process. On one occasion, it took over an hour for a message to get from one OAG terminal through the processing cycle and arrive at another.

The release o OAG-originated and readdressed messages was hampered by previously unknown interface problems between SIGMA and the LDMX. A related problem was the lack of notification to the user when a message was rejected by the LDMX.

The MME Executive Officer, who was fully trained and experienced in SIGMA, was totally occupied in trying to accomplish all the tasks he was supposed to perform during the periods he was working on the MME system. Some of these tasks were not ones that would need to be accomplished in the normal prosecution of an exercise, but were tasks designed to aid in the evaluation of the MME during this particular exercise. At times he was not able to keep up with every task and had to postpone some, such as maintaining the Status of Actions Log or other files containing suspense items. The MME Executive Officer was able to catch up with incoming message distribution in approximately one hour after being absent for an extended period (up to 8-10 hours), because of the low message arrival rate. There were relatively few outgoing messages processed; thus, the MME Executive Officer did not spend much time on this facet of message handling. The MME Executive Officer did spend some time assisting the other OAG users. This would not have been required had all the OAG members been fully trained. The MME Executive Officers agreed that one MME Executive Officer per 12-hour shift would not have been able to handle all the tasks assigned for Power Play 79 if the incoming message flow had been as great as in other exercises. But they felt that if the system's reliability and responsiveness could be improved, the MME system would be of great assistance to the Executive Officers in several of their message-handling tasks.

There were four factors that prevented Exercise Power Play-79 from serving as a satisfactory test for determining the usefulness of an automated message processing system in an exercise/crisis situation. First, CINCPAC participation in the exercise was minimal; second, the MME system was used as the secondary message-processing system on a non-interference basis; third, there were periods during the exercise when a software problem caused excessive system delay; fourth, there were extended periods when the system was down. Further details on PP-79 may be found in [22], the MME Mid-Experiment Report.

7.3.2 Simulated Command Post Exercise (SCPX)

The concept behind the SCPX, which was based on the message traffic archived during PP-79, was to use the MME system as the only message-handling medium for the OAG. The SCPX exercise controller would inject incoming messages into SIGMA; the injection rate could be varied to simulate the normal peaks and valleys of message arrival. Each OAG member had his own terminal and working area in the OAG room. The OAG room was a conference room with seven terminals and a printer multiplexed to one MME connection. The exercise controller and Deputy Crisis Action Coordinator were in separate rooms. Thus, the simulated exercise did not interfere with Command Center Operation and isolated participants from other sources of message traffic. A more complete description of the exercise and the use of the MME system in the exercise is contained in [7].

The message distribution plan for the SCPX differed from that of PP-79. In PP-79, SIGMA sent all incoming messages to the OAG XO, who reviewed each message, made distribution, and assigned action as appropriate. The XO also maintained the Status of Actions Log and the Significant Events Log. In the SCPX, SIGMA filed all messages in the master message file, to which all OAG members had access, and forwarded all messages to the XO. The only requirements for the XO were to review the incoming messages and assign action on them as appropriate and to select items for the Significant Events Log. The Assistant XO (not a participant during PP-79) monitored the Significant Events Log and added comments to each item filed in it by the XO so that any participant could look at the Significant Events Log and see a synopsis of the significant events without having to display each message. The participant had the ability to display and read an entire message if he so desired. Thus, someone could monitor the progress of the exercise on a terminal in his office without having to go to the Command Center (OAG location). The Assistant XO also monitored the Status of Action Log. SIGMA automatically filed a summary in the Status of Actions Log for every message assigned for action by the XO, as well as in the action officer's pending file. When an action officer completed work on a particular message or set of messages, he would make an appropriate comment on the summary in the Status of Actions Log (to which all participants had access). Periodically, the Assistant XO would review the Status of Actions Log and transfer all completed actions to the Action Completed file. Thus, the Status of Actions Log contained only those messages on which action was being taken or had been recently completed.

Action officers were expected to perform as much of their message-handling functions as possible using the terminal, but were free to use the

printer as they desired. Each action officer was expected to review the master file on a periodic basis for messages relating to his functional area. Each action officer's Alert-Selector contained, as a minimum, an entry that would cause an alert whenever he received a message for action. Thus, a summary from the XO would come to his immediate attention. An action officer could retain messages of interest to him either by marking the message with a keyword of his choosing or by creating appropriate files for various messages. Both methods were used during the SCPX. Action officers created outgoing messages and coordinated them within the OAG as required. Each message was then sent to the XO, who checked it and simulated its release by sending it to the controller. The controller double-checked the message, then released it to the LDMX, which provided the drafter a back-copy through SIGMA.

The daily CINCPAC Situation Report (SITREP) was also prepared using SIGMA. Each action officer prepared his portion of the SITREP in a Text Object named Jx-SITREP-INPUT (where the x represented the action officer's OAG code). When an action officer had finished his portion of the SITREP, the J31 representative, who was responsible for the overall SITREP preparation, would GET the text object, VIEW it and COPY the text into the appropriate portion of the In-Preparation SITREP. Once the SITREP was completed, it was processed in the same manner as any other outgoing message.

The SCPX demonstrated that an automated message-handling system as represented by SIGMA is usable in a crisis/exercise situation. The SCPX participants were able to keep up with the incoming message flow (the maximum rate of message input was 30 per hour). They were able to file and retrieve messages in a timely manner. They were able to draft, coordinate, and release outgoing messages, including the SITREP. The backup system devised by the MME staff to provide support in the event of system failure worked satisfactorily.

Messages arrived at each participant's terminal during the SCPX in a rapid manner, regardless of precedence. During PP-79, messages of Immediate and higher precedence were printed directly on the printer in the Command Center by the LDMX at the same time they were delivered to SIGMA by the LDMX. SIGMA delivered Priority and Routine messages to the XO about 30 minutes ahead of the manual system. A principal advantage of an automated system would be the capability to distribute messages selectively to each OAG member, thus relieving him of the need to sort through all the messages to find the ones of interest to him. SIGMA's capability for user-created selectors is a major step in this direction, but because there are no uniform formatting standards for the text portion of military messages, users were not always able to specify selectors that would work as they desired on the text section of messages.

In the manual system, the OAG clerk maintains a master file of all incoming and outgoing messages, generally in time-of-arrival/time-of-dispatch sequence. SIGMA delivered all messages (incoming and back copies of outgoing) to the master file in time-of-arrival (at SIGMA) order. Since in the manual system each OAG member receives a copy of each message, he can create files by subject, originator, etc. (extra copies of paper messages are easily reproduced in the Command Center). SIGMA allows the creation of files by each user and allows each user to mark messages by keywords. The major advantage of the

automated system is the capability for retrieval of messages on multiple parameters, such as user-assigned keywords, subject, originator, date-time group, or any combination thereof. Another advantage is that each user has ready access, through the datefiles, to any previous message concerning his area of interest, even if the message arrived prior to the recognition that a crisis was impending or the start of an exercise. However, unless the user makes a paper copy of each message he needs for reference when composing an outgoing message, he can VIEW only one reference at a time while displaying the In-Preparation message. This makes it awkward if there are several messages to which a user needs to refer in composing his outgoing message. Users in the exercise preferred using SIGMA for filing and retrieving messages.

According to the users, SIGMA provided a good capability for the preparation of outgoing messages, especially for users with adequate typing skills. Users did not have to compete for the services of the OAG clerk-typist when more than one outgoing message needed to be typed, as has been the case in the manual system. The capability of copying sections of text from an object in the view window to the In-Preparation message was very helpful, especially in composing a SITREP. In addition to the obvious saving in time, the copying does not introduce new errors into a message. Coordination of an outgoing message within the OAG was an easy process in both systems. If a message needed to be coordinated outside the OAG, the advantage of the automated system increased as the distance of the coordinator from the Command Center increased. However, if there were off-line references required by the coordinator, the speed advantage of the automated system was sometimes lost. The great majority of OAG messages do not require coordination outside the Command Center; thus, manual coordination does not lag appreciably behind the automated system, especially if off-line references must be obtained anyway. Once a message was approved for release, SIGMA would get it to the LDMX for release to the AUTODIN network faster than the manual system. Manual messages are sent by pneumatic tube from the Command Center to the communications center. The manual message must then be read by the OCR equipment and, if accepted, processed by the LDMX and released to AUTODIN. As noted earlier, a great advantage of SIGMA was the capability to readdress messages and release them rapidly. This was one of the most appreciated features of the automated system.

7.4 Conclusions

Neither the real nor the simulated exercise provided a sufficient environment to make positive judgments concerning the effectiveness of an automated message handling system during a crisis. But some important observations were made during the two exercises that may pertain to the CINCPAC environment and other command centers as well. These observations comparing the previous sytem (the LDMX supplemented by manual procedures) and the new system (the LDMX and SIGMA) are listed below.

(a) Both systems provided a satisfactory message filing and retrieval system. The automated system was faster in retrieving messages that were received prior to the OAG's convening. Depending upon the way the files were set up, a particular message could be found as quickly in the manual system as in the automated system.

(b) The automated system was faster for creating outgoing messages and for readdressals. Coordination required about the same time in both systems. Release was faster by the automated system. All outgoing messages were processed satisfactorily by both systems.

(c) No valid comparison of the quality of outgoing messages produced by the two systems was made.

(d) There is no qualitative difference in message system requirements between crisis/exercise and normal operations. The MME system was easily reconfigured to adapt to the exercises, and the activities conducted by users mirrored those of normal operations. There was, however, a significant increase in message load. Thus the apparent distinction between an automated message-handling system in crisis or normal operations is principally one of throughput.

SECTION 8
IMPLICATIONS FOR FUTURE SYSTEMS

8.1 Introduction

This section presents the conclusions reached as a result of the Military Message Experiment. As noted in Section 1, the major purpose was to determine the utility of a system such as SIGMA in a command environment. Volume IV (ref [8]) of this series discusses the ways of measuring the utility of a system such as the one used for the MME. The real utility of a message handling system in a staff environment is measured by a more efficient response to a critical ACTION message or, more simply, a more efficient overall operation of the staff. This type of utility, of course, is very difficult to quantify, just as the utility of any staff is difficult to quantify. Another difficult question to answer is what is the potential worth of such a system. In other words, given a zero-sum budget, how much should a command invest in a SIGMA-type system? The experiment does not answer this question; rather, it provides information that can be used to determine the characteristics and performance of future systems; then-current computer technology will determine the cost. But the staff officers' reliance on SIGMA during the final part of the experiment and CINCPAC'S attempt to retain the system at the end of the experiment strongly support the conclusion that a military message system is extremely useful in a command environment.

In this section, we present, first, the major conclusions to be drawn from the experiment and, second, the trends and research issues associated with future military message systems.

8.2 Conclusions from the Experiment

(a) An automated message system can be extremely useful in a military environment during both normal and crisis operations (1) by reducing message distribution times, (2) by providing more accurate and efficient distribution and retrieval through user-specified criteria, and (3) by providing word-processing capabilities for generating messages and other documents, thus reducing errors in preparation and release.

For these advantages to be achieved, the system must be extremely reliable and routinely available. Because SIGMA was used interactively, the users demanded more reliability and availability of it than they did of the LDMX.

(b) There are no significant differences between system requirements in normal and crisis operation. During a crisis, the volume of traffic will usually increase; thus, incoming traffic must be filtered so that critical messages can be identified and responded to promptly. An Automated Message Handling System (AMHS) will be effective during a crisis only if the personnel who must use it are thoroughly familiar with its operation. The system should be in daily use and sized to handle worst-case expected traffic loads.

(c) An automated message system must provide services to everyone involved with message handling. Failure to provide adequate coverage will reduce the effectiveness of the organization and will inhibit achieving the level of user proficiency needed for effective use of the system during a crisis. Further, each user may not have a terminal; therefore, the system must have a well thought-out procedure for including these individuals in processes that have been automated (e.g., distribution). The design of the system should consider both users who will usually interface with the system using paper copies and clerk/typists.

(d) An automated message system must have the capability to produce hard copy. In the MME, many users preferred paper copies for reviewing messages and preferred not to use the automated coordination because it did not provide the face-to-face contact that some felt was important.

(e) An automated message system should be an integral part of the user's information handling system. Users who draft messages need to refer to many documents, including other messages, reports, and letters--many of which may be stored on other automated systems. A single workstation is needed to support the user's message-handling, command-and-control, and word-processing functions.

(f) The most likely base for a multilevel-secure message processing system is a security kernel. A security kernel imposes serious restrictions on the functions a user can execute. The experiment shows that, while difficult, it is not impossible to design a user interface for a kernel-based message system that provides the required user capabilities.

(g) A user-oriented message system and the telecommunications center message system with which it is associated must be fully integrated. Otherwise, there will be reduced reliability and increased cost because of incompatible interfaces and duplication of functions. Further, because of the additional capabilities of new systems, the message-handling protocols should be examined for needed changes (e.g., references, key words, and subject line should be under strict format control). See The Quick Look Report [17] for details.

(h) An automated military message system is a more complex program than is generally thought. It must exhibit the characteristics of a well-designed data base system, a user-oriented word processor, an interactive command and control system, and a rapid message handling system. Such a system is further complicated by the need to provide services to a large number of people, the need for certifiably secure operation, the need for Command-defined privacy controls on certain messages and message types, and the need for a user interface that is hospitable to a variety of users. As with any complex computer system, the user interface, security and privacy constraints, performance requirements, and physical hardware often interact in complex ways. A change in one of these may have a detrimental effect on one or more others. For example, the addition of a new function can degrade the user interface, cause a deterioration in performance, or be prohibited because it violates the system's security constraints.

8.3 Implications

(a) Breadth of Coverage. A system must have an adequate number of terminals and printers to be accessible throughout the organization it serves. It must also have the functionality and sufficient processing power to support a critical mass of users. It should be used on a regular basis (e.g. daily) to insure adequate familiarity on the part of the user.

(b) Capacity. A system should be sized to handle worst-case expected traffic loads.

(c) Reliability. The system reliability and availability must approach 100%. Further, it must be perceived by the users as reliable and available. Users who depend on a message processing system to accomplish their required military functions must be provided a system where reliability and availability approach 100% in order for them to have the confidence to depend on it during a crisis.

(d) Architecture. The system must be able to expand gracefully to accommodate additional users or new functions. Alternative architectures based on the use of distributed processing appear to be more appropriate choices than a centralized time sharing system.

(e) Useful Functions. The following are useful in a military message processing system:

handling of informal memos and notes;
rapid scanning in any order of message summaries within a file;
selective retrieval of messages using user-specified criteria;
alerting a user when an important message arrives;
a terminal with multiple windows for viewing related material while composing a message or performing other similar tasks.

(f) Design for Change. The system must be designed so that most user-suggested changes can be incorporated easily.

8.4 Future Directions and Research Issues

(a) The handling of formal military messages will continue to be a combination of manual procedures and automation. In future years, the amount of interactive message handling in the DoD will increase. However, because some message processing tasks cannot be automated easily and because of organizational preferences, certain manual procedures will probably be retained.

(b) The limitations of current large centralized message processing systems coupled with decreasing hardware costs will encourage the development of distributed message system architectures. In some cases, each user's terminal may be powerful enough to act as his own dedicated message processor. These processors will be connected together via local networks.

(c) Although the MME system could only handle text messages, future systems should support new types of messages, such as facsimile, voice, and graphics. Human factors issues, workstation design, and protocols for supporting these new messages should be explored or developed. In addition, new functional capabilities such as automated distribution of messages should be included.

(d) Although there are numerous examples in which privacy controls would be useful, a comprehensive design of privacy controls for military message systems does not exist; such a design should be formulated and tested.

SECTION 9
ACKNOWLEDGEMENTS

The authors acknowledge the contributions to this report by the many people involved in the experiment—in particular, Rob Stotz of USC-ISI, Duane Adams of ARPA, Dave Miller and Sarah Hosmer of MITRE, Norm Thomas of the Naval Electronic Systems Command, Clay Smith of the CINCPAC Staff, Lynn Klitzkie of CTEC, Inc., and Connie Heitmeyer and Janet Stroup of the Naval Research Laboratory.

SECTION 10
REFERENCES

[1] Review of Department of Defense Worldwide Communications, Phase I, Report of the Armed Services Investigating Subcommittee of the Committee on Armed Services, House of Representatives, 92nd Congress, U. S. Govt. Printing Office, May 10, 1971.

[2] Review of Department of Defense Worldwide Communications, Phase II, Report of the Special Subcommittee on Defense Communications of the Committee on Armed Services, House of Representatives, 92nd Congress, H. A. S. C. No. 92-72, U. S. Govt. Printing Office, Oct. 12, 1972.

[3] Review of Department of Defense Worldwide Communications, Phase III, Report of the Special Subcommittee on Defense Communications of the Committee on Armed Services, House of Representatives, 93rd Congress, H. A. S. C. No. 93-76, U. S. Govt. Printing Office, Feb. 7, 1975.

[4] Review of Department of Defense Command, Control and Communications Systems and Facilities, Report by the Command, Control and Communications Panel with a Separate View, Subcommittee on Investigations of the Committee on Armed Services, 94th Congress, H. A. S. C. No. 94-72, U. S. Govt. Printing Office, Feb. 18, 1977.

[5] Memorandum of Agreement between Commander, Naval Telecommunications Command; Commander, Naval Electronic Systems Command; Director, Defense Advanced Research Projects Agency; and Commander in Chief, Pacific, Sep. 1978.

[6] S. H. Wilson, N. C. Goodwin, E. Bersoff, and N. M. Thomas III, MME Final Report Executive Summary, Naval Res. Lab., Washington, D.C., Memorandum Report 4454, March 1982.

[7] C. Smith, MME CINCPAC Final Report, Naval Res. Lab., Washington, D.C., Memorandum Report 4457, Apr. 24, 1981.

[8] R. Jacob, M. Melich, and B. Rudwick, MME - Message System Utility, Naval Res. Lab., Washington, D.C., to be published.

[9] R. Stotz, D. Wilczynski, S. Finkel, R. Lingard, D. Oestreicher, L. Richardson, and R. Tugender, MME - SIGMA Final Report, USC/Inform. Sci. Inst., Marina del Rey, CA, to be published.

[10] N. C. Goodwin and S. W. Hosmer, MME - A User-Oriented Evaluation of Computer-Aided Message Handling, MITRE Corp., Bedford, MA, MTR-3920, Part I, April 1980. Part II, Appendices, MTR-3946, April 1980.

[11] D. G. Miller, MME - Final Training Report, MITRE Corp., Bedford, MA, MTR-3919, May 1980.

[12] E. Bersoff and S. Wilson, Selection Criteria for a Secure Military Message Processing System, Naval Res. Lab., Washington, DC, Memorandum Report 3568, Aug. 1977.

[13] J. Tangney, S. R. Ames, Jr., and E. L. Burke, Security Evaluation Criteria for MME Message Service Selection, MITRE Corp., Bedford, MA, MTR-3433, Jun. 1977.

[14] N. C. Goodwin, S. M. Goheen, and C. Perlingiero, MME Human Factors Evaluation, MITRE Corp., Bedford, MA, M77-207, Sep. 19, 1978.

[15] S. H. Wilson, S. R. Ames, Jr., J. D. Tangney, and J. R. Bunch, Jr., Security/Privacy Evaluation Subcommittee Report on the Candidate Message Service Systems for the Military Message Experiment, Naval Res. Lab., Washington, DC, Report 8155, Sep. 14, 1977.

[16] C. L. Heitmeyer and S. H. Wilson, "Military Message Systems: Current Status and Future Directions," IEEE Transactions on Communications, Vol. Com-27, No. 9, Sept 1980.

[17] S. H. Wilson, J. W. Kallander, N. M. Thomas, III, L. C. Klitzkie, and J. R. Bunch, Jr., MME Quick Look Report, Naval Res. Lab., Washington, DC, Memorandum Report 3992, Apr. 30, 1979.

[18] J. Rothenberg, "On-Line Tutorials and Documentation for the SIGMA Message Service," in Proc. 1979 National Computer Conf., Jun. 4-7, 1979, pp. 863-867.

[19] _____, "SIGMA message service: Reference manual," version 2.3, USC/Inform. Sci. Inst., Marina del Rey, CA, Rep. ISI/TM-78-11.2, Jun. 1979.

[20] R. Stotz, R. Tugender, and D. Wilczynski, "SIGMA - An Interactive Message Service for the Military Message Experiment," in Proc. 1979 National Computer Conf., Jun. 4-7, 1979, pp. 839-846.

[21] R. Stotz, P. Raveling, and J. Rothenberg, "The Terminal for the Military Message Experiment," in Proc. 1979 National Computer Conf., Jun. 4-7, 1979, pp. 855-861.

[22] J. W. Kallander, N. C. Goodwin, S. Hosmer, C. Smith, D. Fralick, L. Klitzkie, and S. H. Wilson, MME Mid-Experiment Report, Naval Res. Lab., Washington, DC, Memorandum Report 4094, Nov. 16, 1979.

[23] S. R. Ames, Jr. and D. R. Oestreicher, "Design of a Message Processing System for a MultiLevel Secure Environment," in Proc. 1978 National Computer Conf., Jun. 5-8, 1978, pp. 765-771.

[24] E. J. McCauley and P. J. Drongowski, "KSOS - The Design of a Secure Operating System," in Proc. 1979 National Computer Conf., Jun. 4-7, 1979, pp. 345-353.

[25] Proposal for the Development of a Multilevel Secure Minicomputer System, Honeywell Avionics Division, St. Petersburg, Fla., Feb. 18, 1977.

[26] R. J. Feiertag and P. G. Neumann, "The Foundations of a Provably Secure Operating System," in Proc. 1979 National Computer Conf., Jun. 4-7, 1979, pp. 329-334.

[27] D. E. Bell and L. J. LaPadula, Secure Computer Systems, Vol. I-II, MITRE Corp., Bedford, MA, MTR-2547, Nov. 1973.

[28] M. A. Padlipsky, K. J. Biba, and R. B. Neely, "KSOS - Computer Network Applications," in Proc. 1979 National Computer Conf., Jun. 4-7, 1979, pp. 373-381.

[29] MME Test Plan forwarded by NAVELEXSYSCOM ltr 310 NMT:lak, Ser: 648:310 of 28 Nov 1978.

[30] N. C. Goodwin, Military Message-Handling Experiment, Baseline Data Report, Test Group, Vol. I, MITRE Corp., Bedford, MA, MTR-3665, Sep. 19, 1978.

[31] C. Weissman, "Security Controls in the ADEPT-50 Time Sharing System," Proc. 1969 AFIPS Fall Jt. Computer Conf., Vol. 35, AFIPS Press, Montvale, N.J., pp. 119-133.

[32] E. I. Organick, The Multics System: An Examination of its Structure, MIT Press, Cambridge, Mass., 1972.

[33] B. D. Gold, R. R. Linde, R. J. Peeler, M. Schaefer, J. F. Scheid, and P. D. Ward, "A Security Retrofit of VM/370," Proc. AFIPS Nat. Computer Conf., Vol. 48, AFIPS Press, Montvale, N. J., 1979, pp.335-342.

[34] GNOSIS External Specifications, Tymshare, Inc., Cupertino, Cal., 1980.

[35] C. E. Landwehr, A Survey of Formal Models for Computer Security, Naval Res. Lab., Washington, DC, Report 8489, Sep. 30, 1981.